Privacy Policy

Last updated January 14, 2026

1. INTRODUCTION

Farther Finance Advisors ("Advisors") is a Delaware limited liability company and a registered investment adviser with the U.S. Securities and Exchange Commission (SEC). Advisors is affiliated with Farther Finance, Inc. (collectively, "Farther", "we", "our", or "us").

Farther is committed to protecting the privacy and security of your personal information. This Privacy Policy describes how we collect, use, share, and protect information about you in connection with our investment advisory services and through our website.

Our Commitment to Your Privacy

Your privacy is not for sale. We do not sell your personal information to anyone, for any reason, at any time. We maintain physical, electronic, and procedural safeguards designed to protect your information in compliance with federal securities laws and regulations, including the Gramm-Leach-Bliley Act and SEC Regulation S-P, as well as California state privacy laws.

2. SCOPE AND APPLICABILITY

This Privacy Policy applies to:

- **Current and prospective clients** of Advisors' investment advisory services
- **Website visitors** who interact with our website
- **Other individual persons** who provide us with personal information or with whom we communicate

Important Distinctions

The privacy protections and rights that apply to you depend on your relationship with us:

Existing Clients (Customers): If you have established an ongoing advisory relationship with Advisors by entering into an investment advisory agreement, you are a "customer" under federal law. Your personal information is protected by the federal Gramm-Leach-Bliley Act (GLBA) and SEC Regulation S-P. For California residents who are existing clients, personal information we collect and use pursuant to GLBA for providing financial services is generally exempt from the California Consumer Privacy Act (CCPA) under the GLBA exemption. However, information collected or used for purposes outside the scope of GLBA (such as marketing or website analytics) remains subject to CCPA. See Section 8.1 for detailed information about the scope of the GLBA exemption.

Prospective Clients: If you have inquired about our services, submitted information through our website, or are considering becoming a client but have not yet entered into an advisory agreement, you are a "prospective client." Information we collect about you before you become a customer is **not** covered by the GLBA exemption and is therefore subject to the California Consumer Privacy Act (CCPA) if you are a California resident, in addition to our comprehensive data security safeguards under federal law.

Website Visitors: If you visit our website without providing personal information or establishing a business relationship, certain information may be collected automatically through cookies and similar technologies as described in Section 11 below.

3. INFORMATION WE COLLECT

To provide investment advisory services and operate our business, we collect various categories of personal information. The specific information we collect depends on your relationship with us and the services you request.

3.1 Categories of Information Collected

Identifiers and Contact Information

- Full legal name, alias, or nickname
- Postal address (residential and business)
- Email address
- Telephone numbers (mobile, home, work)
- Social Security number or Tax Identification Number
- Driver's license number or state identification card number

- Passport number
- Account numbers and online identifiers
- Signature
- Date of birth

Financial Information

- Bank account numbers and routing information
- Investment account numbers and credentials (with your authorization)
- Credit card and debit card numbers
- Financial account information, balances, and transaction history
- Assets, liabilities, income, and expenses
- Net worth and sources of wealth
- Investment holdings and portfolio information
- Credit reports and credit scores
- Tax returns and tax identification information
- Employment information and salary details
- Retirement account information and beneficiary designations

Investment and Advisory Information

- Investment objectives and financial goals
- Risk tolerance and investment experience
- Investment time horizon and liquidity needs
- Tax considerations and tax planning information
- Estate planning information and documents
- Financial planning needs and preferences

Professional and Demographic Information

- Employer name and address
- Job title, position, and work history
- Professional licenses and certifications
- Business contact information
- Age, date of birth, and marital status

- Citizenship status
- Education history and degrees obtained

Sensitive Personal Information

Under federal and California law, certain categories of personal information are considered "sensitive" and receive enhanced protections:

- Social Security number, driver's license number, state identification card number, or passport number
- Financial account numbers in combination with security codes, access codes, or passwords that permit access to an account
- Precise geolocation (if you use our mobile applications with location services enabled)
- Biometric information (such as fingerprints or voice recordings if used for authentication)
- Health information (to the extent relevant for insurance planning)
- Contents of mail, email, or text messages not directed to us
- Genetic data

Internet and Electronic Activity Information

When you visit our website or use our client portal:

- Device information (type, operating system, browser)
- IP address and general location information
- Browsing history and activity on our website
- Search history on our website
- Interaction with our emails and advertisements
- Cookie and tracking technology data
- Login credentials and authentication information

Audio and Visual Information

- Voice recordings of telephone calls with our customer service representatives for quality assurance, training, and security purposes
- Video recordings from security cameras in our offices
- Photographs if provided for identification verification
- Electronic signatures

Professional Inferences

We may develop inferences about you based on the information we collect to create a profile reflecting your investment preferences, financial characteristics, and advisory needs.

3.2 Sensitive Customer Information (Federal Definition)

Under SEC Regulation S-P, "sensitive customer information" means any component of customer information, alone or in combination with other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual. This includes:

- Social Security number
- Driver's license number or government-issued identification number
- Account numbers in combination with security codes or passwords
- Biometric records
- Medical and health information
- Credit or debit card numbers in combination with security codes

We use and disclose sensitive customer information only for purposes permitted by law, such as providing the services you request, preventing fraud, maintaining security, and complying with legal obligations.

4. HOW WE COLLECT INFORMATION

We collect personal information from various sources:

4.1 Directly From You

We collect most personal information directly from you when you:

- Complete account applications, forms, questionnaires, and agreements
- Communicate with us by phone, email, mail, or in person
- Use our website, client portal, or mobile applications

- Provide us with documents, records, and supporting materials
- Submit inquiries through our website contact forms
- Participate in surveys or provide feedback
- Attend our events or webinars

4.2 Automatically From Your Use of Our Services

We automatically collect certain information when you interact with our digital services:

- **Website and Client Portal Usage:** Through cookies, web beacons, and similar technologies, we collect information about your browsing activity, pages viewed, links clicked, and time spent on our website
- **Device Information:** Information about the devices you use to access our services, including IP address, device type, operating system, and browser type
- **Electronic Communications:** Information about whether you open our emails and which links you click

4.3 From Affiliates

We may receive information about you from our affiliated entities if you have relationships with multiple entities within our corporate family or if one affiliate refers you to us.

4.4 From Your Financial Institutions

With your authorization, we collect information about your accounts, holdings, balances, and transactions from:

- Banks and credit unions
- Brokerage firms and custodians
- Investment companies and mutual fund providers
- 401(k) and retirement plan administrators
- Account aggregation services that facilitate access to your financial information

4.5 From Your Professional Advisors

With your consent or at your direction, we may receive information from your:

- Attorneys and estate planning counsel
- Certified Public Accountants (CPAs) and tax preparers
- Insurance agents and brokers
- Other financial advisors

4.6 From Service Providers and Third Parties

We receive information from third-party service providers and vendors, including:

- **Identity Verification Services:** To verify your identity and prevent fraud
- **Consumer Reporting Agencies:** Credit reports and consumer reports (with your authorization and for permissible purposes under the Fair Credit Reporting Act)
- **Data Analytics Providers:** To enhance our understanding of client needs and improve our services
- **Background Check Services:** For compliance and due diligence purposes
- **Fraud Prevention Services:** To detect and prevent fraudulent activity

4.7 From Public Sources

We may obtain information from publicly available sources, including:

- Public records (property records, business registrations, court records)
- News articles and publications
- Databases and registries

4.8 From Referral Sources

We may receive your contact information from:

- Existing clients who refer you to us (with their understanding that you have consented)
- Professional referral networks and strategic partners
- Marketing partners and business development sources

5. HOW WE USE YOUR INFORMATION

We use your personal information for the following business and operational purposes:

5.1 Providing Investment Advisory Services

- Opening and maintaining your investment advisory accounts
- Providing personalized investment advice and portfolio management
- Conducting financial planning and analysis
- Developing and implementing investment strategies tailored to your objectives
- Executing securities transactions on your behalf
- Monitoring and rebalancing your investment portfolios
- Providing ongoing account management and client service

5.2 Servicing Your Account

- Responding to your inquiries, questions, and requests
- Providing customer service and technical support
- Processing transactions, payments, and account changes
- Generating and delivering account statements, confirmations, and reports
- Providing tax reporting documents and year-end summaries
- Communicating with you about your account and our services

5.3 Regulatory Compliance and Legal Obligations

- **SEC and State Registration Requirements:** Complying with our obligations as a registered investment adviser, including maintaining required books and records
- **Anti-Money Laundering (AML) Compliance:** Verifying your identity and conducting customer due diligence to prevent money laundering and terrorist financing
- **Know Your Customer (KYC) Requirements:** Collecting and verifying information to understand your financial situation and investment objectives
- **Tax Reporting:** Preparing and filing required tax reports with federal and state authorities
- **Legal Process:** Responding to subpoenas, court orders, legal process, and government inquiries
- **Regulatory Examinations:** Cooperating with SEC, state, and other regulatory examinations and audits
- **Recordkeeping:** Maintaining records as required by SEC Rule 204-2 and other applicable regulations

5.4 Risk Management and Security

- Detecting, preventing, and investigating fraud, money laundering, and other illegal activities
- Monitoring account activity for suspicious or unauthorized transactions
- Protecting against security threats, cyberattacks, and unauthorized access
- Conducting risk assessments and implementing risk mitigation measures
- Maintaining the security and integrity of our systems and your information
- Conducting internal audits and compliance reviews
- Implementing our incident response program under Regulation S-P

5.5 Business Operations and Analysis

- Processing and fulfilling transactions and service requests
- Managing relationships with service providers and vendors
- Analyzing data to improve our services and develop new offerings
- Conducting market research and understanding client needs
- Evaluating the effectiveness of our advisory strategies
- Performing internal business administration and operations
- Training our employees and maintaining quality assurance

5.6 Communications and Marketing

- Communicating with you about your account, services, and our firm
- Sending educational content, market updates, and investment insights
- Informing you about products, services, and events that may interest you
- Sending newsletters, publications, and thought leadership content
- Marketing our investment advisory services to prospective clients
- Obtaining your feedback through surveys and questionnaires
- Personalizing your experience with our firm

You may opt out of receiving marketing communications at any time by following the unsubscribe instructions in our emails, contacting us at the information provided in Section 14, or adjusting your communication preferences through your account settings.

5.7 Coordinating with Your Other Advisors

With your consent or at your direction, we share information with your other professional advisors, such as:

- Attorneys for estate planning and legal matters
- CPAs and tax preparers for tax planning and preparation
- Insurance agents for insurance planning and implementation
- Other financial advisors when coordinating comprehensive financial strategies

5.8 Website and Technology Functions

- Operating and maintaining our website, client portal, and mobile applications
- Authenticating your identity and providing secure access
- Delivering requested features and functionality
- Analyzing website usage to improve performance and user experience
- Troubleshooting technical issues and providing technical support
- Detecting and preventing fraudulent use of our digital services

6. HOW WE SHARE YOUR INFORMATION

We may share your personal information in the following circumstances. We do not sell your personal information to anyone, for any reason, at any time.

6.1 Sharing with Affiliates

We may potentially share your personal information with our affiliated entities for business purposes, including:

- **Coordinated Services:** To provide services you request from multiple affiliated entities

- **Referrals:** To facilitate referrals among affiliated companies
- **Business Operations:** To conduct consolidated business operations, risk management, and compliance functions
- **Group Services:** To provide centralized services such as information technology, legal, compliance, and human resources

Affiliate Marketing Opt-Out: Under federal law, you have the right to opt out of our affiliated entities using your information to market their products and services to you. If you wish to exercise this right, please contact us using the information in Section 14.

California Residents: For California residents who are existing clients, the GLBA exemption applies to information we collect in connection with providing financial services, and such information is exempt from the CCPA's affiliate sharing restrictions. For prospective clients and website visitors who are California residents, you have rights under the CCPA regarding affiliate sharing as described in Section 8 below.

6.2 Sharing with Service Providers

We share your information with service providers and vendors who perform services on our behalf, including:

- **Custodians and Broker-Dealers:** To hold your assets and execute transactions
- **Account Aggregation Services:** To collect information about your accounts held at other institutions (with your authorization)
- **Technology Providers:** For client relationship management (CRM) systems, portfolio management software, performance reporting tools, and cybersecurity services
- **Cloud Service Providers:** For secure data storage and computing services
- **Administrative Service Providers:** For recordkeeping, document management, and proxy voting services
- **Professional Service Providers:** Legal counsel, auditors, consultants, and compliance professionals
- **Identity Verification and Fraud Prevention Services:** To verify your identity and prevent fraud
- **Communication Services:** Email service providers, mail processing services, and customer communication platforms

Service Provider Requirements: We require all service providers to:

- Implement appropriate administrative, technical, and physical safeguards to protect your information
- Use your information only for the specific purposes for which we engage them
- Notify us within 72 hours if they become aware of unauthorized access to or use of your information
- Comply with applicable privacy and security laws

We conduct due diligence before engaging service providers and perform ongoing oversight to ensure they maintain appropriate safeguards for your information.

6.3 Sharing with Your Consent or At Your Direction

We share your information when you have provided consent or directed us to do so, including:

- Sharing information with your spouse, family members, or other designated individuals
- Coordinating with your other professional advisors as described in Section 5.7
- Fulfilling specific requests you make to share information with third parties
- Providing information to joint account holders and authorized representatives

6.4 Sharing for Legal and Regulatory Purposes

We may disclose your information when required or permitted by law, including:

- **Legal Compliance:** To comply with applicable laws, regulations, and legal obligations
- **Regulatory Requests:** In response to requests from the SEC, state securities regulators, FINRA, or other regulatory authorities
- **Legal Process:** Pursuant to subpoenas, court orders, warrants, or other legal process
- **Law Enforcement:** To cooperate with law enforcement investigations
- **Protection of Rights:** To protect our rights, property, safety, or the rights, property, and safety of our clients, employees, or others
- **Fraud Prevention:** To detect, prevent, and investigate fraud, money laundering, and other illegal activities

6.5 Sharing for Business Transactions

We may share your information in connection with a corporate transaction, including:

- Merger, acquisition, or sale of assets
- Corporate reorganization or restructuring
- Bankruptcy or insolvency proceedings
- Due diligence related to any of the above

In such cases, we will require the acquiring or successor entity to honor the commitments made in this Privacy Policy.

6.6 Exceptions Under Federal Law

Under the Gramm-Leach-Bliley Act and its implementing regulations, we may share your nonpublic personal information with nonaffiliated third parties without providing you an opportunity to opt out in the following circumstances:

- As necessary to effect, administer, or enforce a transaction you request or authorize
- To maintain or service your account
- In connection with processing or servicing a financial product or service you request
- In connection with maintaining or servicing your account with us or with another entity as part of a private label credit card program or similar extension of credit
- To resolve consumer disputes or inquiries
- To comply with federal, state, or local laws, rules, and legal requirements
- To comply with a properly authorized civil, criminal, or regulatory investigation or subpoena
- To report to consumer reporting agencies
- To report to government entities for fraud prevention purposes
- For institutional risk control or resolving customer disputes
- To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability
- For required institutional risk control or for resolving customer disputes or inquiries
- To protect the confidentiality or security of our records

6.7 Aggregate and De-Identified Information

We may share aggregate, de-identified, or anonymized information that does not identify you personally for research, analysis, marketing, and other business purposes. Such information is not considered personal information under applicable privacy laws.

6.8 What We Do Not Do With Your Information

To emphasize our commitment to your privacy:

- **We do not sell your personal information** to anyone, for any reason, at any time
- **We do not rent or lease your personal information** to third parties for their marketing purposes
- **We do not share your information with nonaffiliated third parties for marketing purposes** unless you have provided consent (California residents must provide opt-in consent under state law)

- **We do not share your account numbers** with nonaffiliated third parties for marketing purposes

7. YOUR PRIVACY RIGHTS AND CHOICES

7.1 Opt-Out Rights Under Federal Law

Nonaffiliated Third-Party Sharing: Federal law generally requires that we provide you with the opportunity to opt out before we share your nonpublic personal information with nonaffiliated third parties, except as permitted by law (see Section 6.6). Currently, we do not share your information with nonaffiliated third parties for marketing purposes outside the permissible exceptions.

Affiliate Marketing: You have the right to opt out of our affiliated entities using your information (such as information about your creditworthiness) to market their products and services to you. To exercise this opt-out right, contact us using the information in Section 14.

7.2 Annual Privacy Notice Exception

Under federal law, financial institutions that meet certain conditions are not required to provide annual privacy notices to customers. Advisors qualifies for this exception because we:

- Share nonpublic personal information only under the exceptions permitted by Sections 13, 14, and 15 of Regulation S-P
- Have not changed our policies and practices regarding disclosure of nonpublic personal information from those most recently disclosed to you

If our practices change such that we no longer qualify for this exception, we will provide you with an updated privacy notice before implementing the change.

7.3 Communication Preferences

Marketing Communications: You may opt out of receiving marketing emails, newsletters, and promotional communications from us at any time by:

- Clicking the "unsubscribe" link at the bottom of our marketing emails
- Contacting us at privacy@farther.com

- Adjusting your communication preferences in your account settings

Important Account Communications: Even if you opt out of marketing communications, we will continue to send you important account-related communications, such as account statements, confirmations, tax documents, regulatory notices, and service-related announcements.

7.4 Accessing and Updating Your Information

You may access and update your personal information by:

- Logging into your secure client portal
- Contacting your dedicated financial advisor
- Emailing us at privacy@farther.com
- **Sending mail to** Farther Finance Advisors, LLC, Attention: Privacy Officer, [345 California St, Ste 600, San Francisco, CA 94104]

We encourage you to keep your information current and accurate. Please notify us promptly of any changes to your contact information, financial circumstances, investment objectives, or other material information that may affect our advisory relationship.

7.5 Credit Report Rights

Obtaining Consumer Reports: We may obtain consumer reports about you from consumer reporting agencies (such as credit reports) for permissible purposes under the Fair Credit Reporting Act, including to verify information you provide and to evaluate applications for financial products and services.

Adverse Action Notices: If we take adverse action based in whole or in part on information contained in a consumer report, we will provide you with written notice that includes:

- The name, address, and telephone number of the consumer reporting agency that provided the report
- A statement that the consumer reporting agency did not make the adverse decision and cannot explain why the decision was made
- Your right to obtain a free copy of your consumer report from the agency within 60 days
- Your right to dispute the accuracy or completeness of information in the report

Free Annual Credit Reports: You have the right to obtain a free credit report once every 12 months from each of the three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion) by visiting www.annualcreditreport.com or calling 1-877-322-8228.

8. CALIFORNIA PRIVACY RIGHTS

This section applies to California residents and describes rights provided under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), and other California privacy laws.

8.1 Application of the CCPA to Farther

GLBA Exemption: The CCPA provides a limited exemption for personal information that is collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801 et seq., and its implementing regulations. As a registered investment adviser, Advisors is subject to GLBA. However, this exemption is activity-based and purpose-specific, not a blanket exemption for all information about our clients.
Understanding the Scope of the GLBA Exemption:

The GLBA exemption applies only to personal information that we collect, process, or disclose for purposes directly related to:

- Providing financial products or services to you as required or authorized under GLBA

- Activities necessary to effect, administer, or enforce transactions you request or authorize

- Maintaining or servicing your account with us

- Complying with GLBA's own privacy, safeguarding, and regulatory requirements

The GLBA exemption does NOT apply to personal information we collect or use for purposes outside the scope of GLBA, including but not limited to:

- Marketing and advertising activities (except as specifically permitted under GLBA)

- Website analytics and user experience optimization

- General business operations not directly related to providing financial services

- Employment-related decisions or background checks

- Social media interactions and engagement - Market research and product development

Application to Different User Categories:

Existing Clients (Customers): If you are an existing client with an ongoing advisory relationship with Farther Finance Advisors:

- Personal information we collect and use pursuant to GLBA for providing investment advisory services, maintaining your account, and complying with financial services regulations is generally exempt from the CCPA under the GLBA exemption.

- However, personal information we collect or use for purposes outside the scope of GLBA (such as website browsing behavior, marketing preferences, or information collected through cookies for advertising purposes) remains subject to the CCPA, and you retain CCPA rights with respect to such information.

Prospective Clients: If you are a prospective client who has inquired about our services or submitted information through our website but have not yet entered into an advisory agreement:

- The information we collect about you before you become a customer is generally not covered by the GLBA exemption because we do not yet have a customer relationship with you for purposes of providing financial services.

- Therefore, if you are a California resident, such information is subject to the CCPA, and you have the full range of rights described in Section 8.2 below.

Website Visitors: If you visit our website without providing personal information or establishing a business relationship:

- Information collected through cookies, analytics, and similar technologies is subject to the CCPA (for California residents) because it is not collected pursuant to GLBA.

- You have the rights described in Section 8.2 below, including the right to opt out of the sale or sharing of your personal information.

Important Note About Mixed-Purpose Information:

Some personal information may be collected or used for both GLBA-covered purposes and non-GLBA purposes. For example:

- Your email address may be used both to send you account statements (GLBA-covered) and marketing newsletters (not GLBA-covered)

- Your browsing activity on our client portal may be used both to provide secure account access (GLBA-covered) and to analyze user experience for marketing purposes (not GLBA-covered)

When information is used for mixed purposes, the GLBA exemption applies only to the GLBA-covered uses. For non-GLBA uses, California residents retain their CCPA rights.

Transition from Prospective Client to Customer:

Once you become a customer by entering into an investment advisory agreement:

- Information we collect going forward in connection with providing financial services pursuant to GLBA becomes subject to the GLBA exemption (to the extent used for GLBA-covered purposes)

- Information collected before you became a customer may continue to be subject to CCPA for its original collection purposes

- Information collected or used for non-GLBA purposes after you become a customer remains subject to CCPA

If you have questions about whether specific information or uses are covered by the GLBA exemption, please contact our Privacy Officer at privacy@farther.com.

8.2 California Consumer Rights

If you are a California resident and your information is not subject to the GLBA exemption (e.g., you are a prospective client or website visitor), you have the following rights under the CCPA:

Right to Know

You have the right to request that we disclose to you:

- The categories of personal information we have collected about you
- The categories of sources from which the personal information was collected
- The business or commercial purposes for collecting, selling, or sharing personal information
- The categories of third parties to whom we disclose personal information
- The specific pieces of personal information we have collected about you

You may submit a request to know up to twice in a 12-month period.

Right to Delete

You have the right to request that we delete personal information we have collected from you, subject to certain exceptions. We may retain personal information as necessary to:

- Complete the transaction for which the information was collected, provide a service you requested, or perform under a contract with you
- Detect and resolve security incidents and protect against malicious, deceptive, fraudulent, or illegal activity
- Debug to identify and repair errors
- Comply with legal obligations
- Use the information internally in ways that are compatible with the context in which you provided it or that are reasonably aligned with your expectations

Right to Correct

You have the right to request that we correct inaccurate personal information we maintain about you. We will use commercially reasonable efforts to correct the information as directed by you.

Right to Opt-Out of Sale or Sharing

You have the right to opt out of the "sale" or "sharing" of your personal information. Under the CCPA:

- **"Selling"** means disclosing personal information to a third party for monetary or other valuable consideration
- **"Sharing"** means disclosing personal information to a third party for cross-context behavioral advertising (also known as targeted advertising)

Our Practice: We do not sell your personal information in exchange for money. However, when you visit our website, we may disclose certain categories of personal information to third-party advertising and analytics partners through cookies and similar technologies. Under the CCPA, these disclosures may be considered a "sale" or "sharing" of personal information even though we do not receive monetary compensation.

Specific Information That May Be "Sold" or "Shared":

The following table describes the categories of personal information we may disclose in ways that could constitute "sale" or "sharing" under the CCPA, the purposes for such disclosures, and the categories of third parties who may receive the information:

Category of Personal InformationPurpose of DisclosureCategories of Third PartiesIdentifiers:

- IP addresses
- Device identifiers
- Cookie IDs
- Mobile advertising IDs
- Browser fingerprints- Targeted advertising
- Marketing campaign measurement
- Audience analytics

Cross-device tracking

- Retargeting/remarketing- Advertising networks (e.g., Google Ads, Facebook/Meta)
- Social media platforms (e.g., LinkedIn, Facebook, Twitter/X)
- Analytics providers (e.g., Google Analytics)
- Marketing technology platforms Internet/Network Activity:
- Pages viewed- Links clicked
- Time spent on pages
- Referring URLs
- Search queries on our site - Website optimization
- User experience analysis

- Conversion tracking

- A/B testing

- Behavioral advertising- Analytics providers

- Advertising networks

- Marketing platforms

- Heat mapping services Geolocation Data:

- General location (city/state)

- Derived from IP address (not precise geolocation) - Geographic targeting

- Localized content- Regional marketing - Advertising networks

- Analytics providers Inferences:

- Interests

- Preferences

- Behavioral predictions - Interest-based advertising

- Audience segmentation

- Predictive modeling - Advertising networks

- Data analytics companies

- Marketing platforms

Important Clarifications:

- We do NOT sell or share sensitive personal information such as Social Security numbers, financial account numbers, precise geolocation, health information, or account passwords.

- We do NOT sell or share personal information of existing clients that we collect in connection with providing investment advisory services (this information is generally subject to the GLBA exemption as described in Section 8.1).

- The "sale" or "sharing" described above primarily involves prospective clients and website visitors, and relates to information collected through our website for marketing and analytics purposes.

- We do NOT sell or share personal information of individuals we know are under 18 years of age.

Specific Third-Party Services We Use:

To provide additional transparency, we currently use the following third-party services that may

receive personal information in ways that constitute "sale" or "sharing":

- Google Ads

- Meta Ads

- LinkedIn Ads

This list may change over time as we add or remove marketing and analytics services. For the most current list, please contact us at privacy@farther.com.

To Opt Out:

1. Click the "**Do Not Sell or Share My Personal Information**" link on our website homepage
2. Adjust your cookie preferences in our cookie banner
3. Enable Global Privacy Control (GPC) in your browser (we honor GPC signals)
4. Contact us at privacy@farther.com

Right to Limit Use of Sensitive Personal Information

You have the right to limit our use and disclosure of your sensitive personal information to:

- Uses necessary to perform the services or provide the goods you reasonably expect
- Uses specified in CCPA regulations, including preventing fraud, ensuring security, processing transactions, and complying with legal obligations

Our Practice: We use and disclose sensitive personal information only for purposes permitted by law and for which you would reasonably expect us to use such information in connection with our investment advisory services.

Right to Non-Discrimination

You have the right not to receive discriminatory treatment for exercising your CCPA privacy rights. We will not:

- Deny you goods or services
- Charge you different prices or rates for goods or services
- Provide you a different level or quality of goods or services
- Suggest that you may receive a different price or rate or level or quality of goods or services

8.3 How to Exercise Your California Rights

To exercise your rights to know, delete, or correct, you may:

- **Submit a Request Online:** Click on “Your Privacy Choices” link at the bottom of the site and opt-out.
- **Email Us:** privacy@farther.com with "California Privacy Request" in the subject line
- **Mail Us:** Farther Finance Advisors, LLC, Attention: Privacy Officer, 345 California St, Ste 600, San Francisco, CA 94104

Verification: To protect your privacy and security, we will verify your identity before processing your request. We may request additional information from you, such as your name, email address, phone number, and information about your relationship with us. The verification process may differ depending on the nature of your request and the sensitivity of the information requested.

Authorized Agents: You may designate an authorized agent to submit requests on your behalf. The authorized agent must provide proof of authorization, and we may require you to verify your identity directly with us and confirm that you provided the agent permission to submit the request.

Response Timeframe: We will respond to verifiable requests within 45 days of receipt. If we require more time (up to an additional 45 days), we will inform you of the reason and extension period in writing. We will deliver our written response electronically unless you request a different method.

No Fee: We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will provide you with a cost estimate and explanation before completing your request.

8.4 California Shine the Light Law

California Civil Code Section 1798.83 permits California residents to request certain information about our disclosure of personal information to third parties for their direct marketing purposes. We do not disclose your personal information to third parties for their direct marketing purposes unless you provide opt-in consent as required by California law.

8.5 California Financial Information Privacy Act (CFIPA)

California Financial Code Sections 4050-4060 provide additional privacy protections for California residents. Under CFIPA, we will not share your nonpublic personal information with nonaffiliated third parties for marketing purposes unless we obtain your separate written consent.

Opt-In Consent Requirement: Before we share your financial information with a nonaffiliated company for their marketing purposes, we will provide you with a separate consent form that:

- Is a stand-alone document
- Clearly discloses that you are consenting to the sharing
- Explains that the consent remains in effect until revoked
- Describes your right to revoke consent at any time
- Provides the procedure for revoking consent

Revocation: You may revoke your consent at any time by contacting us at privacy@farther.com.

8.6 California Data Breach Notification

California law requires that we notify California residents of data breaches involving personal information. Under California Civil Code § 1798.82, as amended by Senate Bill 446 (effective January 1, 2026), we will notify affected California residents in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The notification will include:

- A description of the breach
- The types of personal information involved
- Steps we are taking in response
- Contact information for questions

- Resources available to protect yourself, such as instructions for obtaining credit reports and placing fraud alerts or security freezes

Notification Timing Standards:

- Primary Standard: We will provide notification "in the most expedient time possible and

without unreasonable delay." This means we will notify you as quickly as we can

reasonably do so after discovering the breach and completing our initial assessment.

- Maximum Timeframe: We aim to provide notification no later than 30 calendar days

after we discover or are notified of the breach, unless a longer delay is specifically

required by law enforcement.

- Discovery Defined: For purposes of California law, we "discover" or are "notified of" a

breach when we determine or have a reasonable basis to determine that unencrypted or

unredacted personal information was, or is reasonably believed to have been, acquired by

an unauthorized person.

Attorney General Notification:

If the breach affects 500 or more California residents, we will aim to submit a sample copy of the breach notification to the California Attorney General within 15 calendar days of notifying affected individuals, as permitted by California law.

The Attorney General submission will include the sample notice and may include additional

information about the breach as required by the Attorney General's office.

8.7 Global Privacy Control (GPC)

We recognize and honor Global Privacy Control (GPC) signals. GPC is a browser-based signal that communicates your opt-out preference for the sale or sharing of your personal information. If your browser or browser extension sends a GPC signal, we will treat it as a valid request to opt out of the sale or sharing of your personal information collected through our website

To enable GPC:

- Use a browser that supports GPC (such as Firefox, Brave, or DuckDuckGo)
- Install a browser extension that enables GPC
- Enable the GPC setting in your browser or extension settings

9. DATA SECURITY

Protecting your personal information is a top priority. We have implemented comprehensive administrative, technical, and physical safeguards designed to protect customer information from unauthorized access, use, disclosure, alteration, and destruction.

9.1 Safeguards Program

Our safeguards program includes:

Administrative Safeguards:

- Designation of employees responsible for coordinating our information security program
- Regular risk assessments to identify reasonably foreseeable internal and external threats
- Security policies and procedures that are reviewed and updated regularly
- Employee training on data security, privacy, and confidentiality obligations
- Background checks and confidentiality agreements for employees
- Role-based access controls limiting employee access to information on a need-to-know basis
- Monitoring and testing of safeguards effectiveness

Technical Safeguards:

- Encryption of sensitive data in transit and at rest using industry-standard encryption protocols
- Multi-factor authentication for remote access to systems

- Firewalls, intrusion detection systems, and intrusion prevention systems
- Regular vulnerability assessments and penetration testing
- Secure network architecture and segmentation
- Antivirus and anti-malware software
- Secure software development practices
- Regular security patches and updates
- Data loss prevention technologies

Physical Safeguards:

- Secure facilities with controlled physical access
- Video surveillance and alarm systems
- Visitor management and escort procedures
- Secure storage of physical records in locked cabinets and rooms
- Clean desk and clear screen policies
- Secure disposal of physical records through shredding or destruction
- Protections for laptops, mobile devices, and removable media
- Environmental controls to protect equipment and data

9.2 Incident Response Program

As required by SEC Regulation S-P, we have established and maintain a written incident response program designed to detect, respond to, and recover from unauthorized access to or use of customer information. Our incident response program includes:

Detection and Assessment:

- Procedures to assess the nature, scope, and cause of any incident
- Identification of customer information that may have been accessed or used without authorization
- Determination of whether sensitive customer information was or is reasonably likely to have been accessed or used without authorization

Containment and Mitigation:

- Procedures to contain and control the incident to prevent further unauthorized access or use
- Immediate actions to secure systems and protect customer information

- Coordination with law enforcement, regulators, and cybersecurity experts as appropriate

Notification:

- Procedures for notifying affected individuals whose sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization
- Notification to regulators as required by law
- Coordination with service providers regarding their notification obligations

Recovery and Remediation:

- Procedures to restore the reasonable integrity of the affected information systems
- Implementation of additional safeguards to prevent recurrence
- Post-incident review and lessons learned
- Updates to policies and procedures based on incident findings

9.3 Service Provider Oversight

We maintain written policies and procedures for overseeing service providers who have access to or maintain customer information. Our service provider oversight includes:

- **Due Diligence:** Conducting due diligence before engaging service providers to assess their ability to maintain appropriate safeguards
- **Contractual Requirements:** Requiring service providers by contract to implement and maintain administrative, technical, and physical safeguards to protect customer information
- **Periodic Assessment:** Conducting periodic assessments of service providers' safeguards and compliance
- **Incident Notification:** Requiring service providers to notify us as soon as possible, and no later than 72 hours, after the service provider becomes aware of any incident involving unauthorized access to or use of customer information that the service provider maintains or otherwise processes on our behalf. For purposes of this requirement:
    - "Becomes aware" means the point at which the service provider has a reasonable basis to conclude that an unauthorized access or use has occurred
    - The 72-hour period begins when the service provider becomes aware, not when the incident initially occurred
    - "As soon as possible" means the service provider must notify us without unreasonable delay, even if the full scope of the incident is not yet known
    - Service providers must provide initial notification within 72 hours even if their investigation is ongoing, and must provide updated information as it becomes available

- Our service provider contracts include specific notification procedures, escalation contacts, and required information to be included in incident notifications
- Failure to provide timely notification is considered a material breach of the service provider agreement and may result in contract termination and liability for resulting damages

Service Provider Incident Response Coordination: When a service provider notifies us of an incident, we aim to do the following:

- Immediately assess whether the incident involves sensitive customer information as defined in Regulation S-P

- Determine whether notification to affected individuals is required

- Coordinate with the service provider to contain and remediate the incident

- Require the service provider to preserve evidence and cooperate with our investigation

- Evaluate the service provider's incident response and determine whether continued engagement is appropriate

We maintain a service provider incident response playbook that includes specific procedures, escalation protocols, and decision trees for responding to service provider incidents. This playbook is reviewed and updated at least annually and after any significant incident.

9.4 Data Breach Notification

In the event of a data breach involving your sensitive customer information, we will notify you in accordance with applicable federal and state laws:

Federal Requirements (SEC Regulation S-P): We will notify affected individuals as soon as practicable, but not later than **30 days** after we have a reasonable basis to conclude that

unauthorized access to or use of sensitive customer information has occurred, or is reasonably

likely to have occurred, that could result in substantial harm or inconvenience to an affected

individual.

Determining When We "Become Aware": For purposes of the 30-day notification deadline, we "become aware" of an incident when we have a reasonable basis to conclude that an unauthorized access or use has occurred. This determination is based on:

- The nature and scope of the incident

- The types of sensitive customer information involved

- Whether the information was actually acquired or accessed by an unauthorized person

- The likelihood of harm to affected individuals

Law Enforcement Delay: The 30-day notification period may be delayed if a law enforcement agency determines that notification will impede a criminal investigation or cause damage to national security. In such cases:

- We will cooperate with law enforcement's reasonable requests for delay

- We will notify affected individuals as soon as law enforcement determines that notification will no longer impede the investigation

- We will document any law enforcement requests for delay

If notification is delayed at the request of law enforcement, we will provide notification promptly after law enforcement advises that notification will no longer compromise the investigation.

California Requirements (SB 446, effective January 1, 2026): For California residents, we aim to provide notification within **30 calendar days** of discovery of a breach. If the breach affects 500 or more California residents, we may also notify the California Attorney General within **15 calendar days** of notifying individuals.

Notification Content: Our data breach notification will include:

- A description of the incident and when it occurred
- The types of sensitive customer information involved
- Steps we are taking in response to the incident

- Contact information for you to ask questions or obtain more information
- Resources available to you to protect yourself, including:
    - Toll-free telephone numbers for major consumer reporting agencies
    - Instructions for obtaining fraud alerts and security freezes
    - Information about the FTC's identity theft resources

Delayed Notification: Notification may be delayed only to:

- Accommodate the legitimate needs of law enforcement
- Determine the scope of the breach
- Restore the reasonable integrity of our data systems

9.5 Secure Disposal

We properly dispose of customer information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Our disposal procedures include:

- Shredding or destroying paper documents containing sensitive information
- Securely deleting or wiping electronic files and media
- Degaussing or physically destroying hard drives and storage devices
- Using certified disposal vendors with contractual confidentiality obligations
- Maintaining records of disposal activities

9.6 Limitations

While we implement comprehensive safeguards, no security system is impenetrable. We cannot guarantee the absolute security of your information, and we cannot be responsible for security breaches caused by factors beyond our reasonable control, such as:

- Your own actions or the actions of others with whom you share your login credentials
- Inherent risks of internet and email transmission
- Vulnerabilities in third-party software or services
- Sophisticated cyberattacks that circumvent security measures

Your Role in Security: You play an important role in protecting your information:

- Keep your login credentials confidential and do not share them with anyone
- Use strong, unique passwords and change them regularly
- Enable multi-factor authentication where available
- Be cautious of phishing emails and suspicious communications
- Keep your devices and software updated with the latest security patches
- Notify us immediately if you suspect unauthorized access to your account
- Use secure internet connections and avoid public Wi-Fi for accessing your account

10. DATA RETENTION

We retain your personal information for as long as necessary to fulfill the purposes described in this Privacy Policy, comply with our legal and regulatory obligations, resolve disputes, enforce our agreements, and maintain business operations.

10.1 Retention Periods

Customer Information: For existing clients (customers), we retain your information for the duration of our advisory relationship and for a period of time after the relationship ends as required by law and necessary for our legitimate business purposes. Under SEC regulations, registered investment advisers are generally required to maintain books and records, including customer information, for at least **six years** after the end of the fiscal year in which the last entry was made.

Prospective Client Information: For prospective clients who do not become customers, we retain your information for a reasonable period to respond to your inquiries and maintain records of our interactions, and as required for our business operations and legal compliance.

Website Visitor Information: Information collected through cookies and similar technologies is retained in accordance with our Cookie Policy (see Section 11).

Legal Hold: We may retain information for longer periods when required by law, regulation, or legal hold, or when necessary for litigation, investigations, or dispute resolution.

10.2 Deletion Requests

If you are a California resident and your information is subject to the CCPA (*e.g.*, prospective client or website visitor), you may request deletion of your personal information as described in Section 8. However, we may retain information as permitted by law for the purposes described in Section 10.1.

Upon termination of our advisory relationship, we will retain your information as required by law and for legitimate business purposes, including:

- Complying with our recordkeeping obligations under SEC regulations
- Responding to regulatory examinations and inquiries
- Defending against claims or litigation
- Maintaining archives and backup systems
- Complying with tax and accounting requirements

11. COOKIES AND TRACKING TECHNOLOGIES

Our website uses cookies, web beacons, pixels, and similar tracking technologies to enhance your experience, analyze website usage, and deliver relevant content and advertisements.

11.1 What Are Cookies?

Cookies are small text files stored on your device when you visit a website. They allow the website to recognize your device and remember information about your visit, such as your preferences and login status.

11.2 Types of Cookies We Use

Strictly Necessary Cookies: These cookies are essential for our website to function and cannot be disabled. They enable core functionality such as security, network management, authentication, and accessibility. Without these cookies, services you request cannot be provided.

Performance and Analytics Cookies: These cookies collect information about how you use our website, such as which pages you visit and whether you encounter errors. This information is aggregated and anonymous and helps us improve the performance and usability of our website. We use services such as Google Analytics for this purpose.
Functionality Cookies: These cookies allow our website to remember choices you make (such as your username, language, or region) and provide enhanced, personalized features. They may also be used to provide services you request, such as watching a video or commenting on content.
Targeting and Advertising Cookies: These cookies track your browsing activity across websites and are used to deliver advertisements that are relevant to you and your interests. They may be set by us or by third-party advertising partners. They also help measure the effectiveness of advertising campaigns.

11.3 Third-Party Cookies and Analytics

We use third-party services to analyze website traffic and user behavior:
Google Analytics: We use Google Analytics to understand how visitors use our website. Google Analytics collects information such as how often users visit our website, what pages they visit, and what other websites they used prior to coming to our website. Google Analytics uses cookies and may collect IP addresses and other device identifiers. For more information about Google Analytics, visit https://www.google.com/policies/privacy/partners/. You can opt out of Google Analytics by installing the Google Analytics Opt-Out Browser Add-on available at https://tools.google.com/dlpage/gaoptout.
Advertising and Marketing Partners: We may work with third-party advertising and analytics partners who use cookies and similar technologies to collect information about your browsing activity for the purpose of delivering targeted advertisements and measuring the effectiveness of our marketing campaigns. This may include services such as Google Ads, Facebook Pixel, LinkedIn Insight Tag, and other advertising platforms.

11.4 Your Cookie Choices

Notice of Cookie Use:

When you first visit our website, we display a notice in the footer informing you that we use cookies for essential site functionality, analytics, personalization, and targeted advertising. This notice includes a link to this Privacy Policy and a link to exercise your right to opt out of the sale or sharing of your personal information.
How Cookies are Deployed:

- Strictly Necessary Cookies: Cookies essential for website functionality (such as security, authentication, and load balancing) are deployed automatically. These cookies are necessary to provide services you request and do not require consent under applicable law because they are necessary to provide services you request.

- Non-Essential Cookies: We deploy performance, functionality, and targeting/advertising cookies to improve your experience and deliver relevant content. You may opt out of the sale or sharing of your personal information collected through these cookies as described below.

Managing Your Cookie Preferences:

You can manage cookies in the following ways:

- Opt Out of Sale/Sharing: California residents may click the "Do Not Sell or Share My Personal Information" link in our website footer to opt out of the sale or sharing of personal information collected through cookies and similar technologies.

- Browser Settings: You can configure your browser to refuse cookies or alert you when cookies are being sent. If you disable cookies, some features of our website may not function properly. Instructions for managing cookies in popular browsers:

- Chrome: https://support.google.com/chrome/answer/95647
- Firefox: https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer
- Safari: https://support.apple.com/guide/safari/manage-cookies-and-website-data-sfri11471/mac
- Edge: https://support.microsoft.com/en-us/microsoft-edge/delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09

- Industry Opt-Out Tools: You can opt out of interest-based advertising from participating companies through:

  - Digital Advertising Alliance (DAA): http://optout.aboutads.info
  - Network Advertising Initiative (NAI): http://optout.networkadvertising.org

Global Privacy Control (GPC): We honor Global Privacy Control signals. If your browser sends a GPC signal, we will treat it as an opt-out request for the sale or sharing of your personal information through cookies and tracking technologies. See Section 8.7 for more information about GPC.

Do Not Track (DNT): Some browsers have a "Do Not Track" feature that lets you tell websites that you do not want your online activities tracked. At this time, there is no universal standard for how DNT signals should be interpreted. We do not currently respond to DNT signals, but we do honor GPC signals as described above.

Important Information:

- If you clear your browser cookies, any opt-out preferences stored in cookies will be deleted.

- If you use multiple devices or browsers, you will need to manage your preferences separately on each.

- Private/incognito browsing sessions do not retain cookie preferences.

11.5 Mobile Applications

If we offer you a mobile application, please note the application may use tracking technologies to collect information about your device and usage. You can control some data collection through your device settings:

- **Location Services:** You can disable location services through your device settings
- **Advertising Identifiers:** You can reset or limit ad tracking through your device settings (iOS: Settings > Privacy > Advertising; Android: Settings > Google > Ads)
- **Push Notifications:** You can disable push notifications through your device settings or the app settings

12. CHILDREN'S PRIVACY

Our investment advisory services and website are not directed to individuals under the age of 18, and we do not knowingly collect personal information from children under 18. If we become aware that we have inadvertently collected personal information from a child under 18, we will take steps to delete such information from our records. If you believe we may have collected information from a child under 18, please contact us immediately at privacy@farther.com.

Custodial Accounts: We may collect personal information about minors in connection with custodial accounts established under the Uniform Transfers to Minors Act (UTMA) or Uniform Gifts to Minors Act (UGMA). In such cases, we collect and use the minor's information only as necessary to provide the services requested by the custodian and in accordance with applicable legal requirements.

13. CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, services, legal requirements, or for other operational, legal, or regulatory reasons. When we make changes, we will update the "Last Updated" date at the top of this Privacy Policy and post the updated policy on our website.

13.1 Notice of Material Changes

Existing Clients: If we make material changes that significantly affect your privacy rights or how we use your information, we will notify you by:

- Sending you an email notification to the email address on file (if you have provided one)
- Posting a prominent notice on our website before the changes take effect
- Providing a copy of the updated privacy policy with your next account statement

Prospective Clients and Website Visitors: We will post the updated privacy policy on our website. Material changes will be indicated by a notice on our homepage or in our cookie banner.

13.2 Your Continued Use

Your continued use of our services or website after we post changes to this Privacy Policy constitutes your acceptance of the updated policy. We encourage you to review this Privacy Policy periodically to stay informed about how we protect your information.

13.3 Previous Versions

Previous versions of this Privacy Policy may be available upon reasonable written request by contacting us at privacy@farther.com.

14. CONTACT INFORMATION

If you have questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us:

Farther Finance Advisors, LLC

Attention: Privacy Officer

345 California St, Ste 600

San Francisco, CA 94104

Email:

privacy@farther.com

Website:

www.farther.com

For California Privacy Requests:

+1-628-246-8004

Email: privacy@farther.com (Subject: "California Privacy Request")

14.1 Privacy Officer

We have designated a Privacy Officer responsible for overseeing our privacy program and ensuring compliance with applicable privacy laws. Our Privacy Officer is available to answer your questions and address your concerns about our privacy practices.

14.2 Response Time

We will make every effort to respond to your inquiries and requests promptly. For California privacy requests, we will respond within 45 days as required by applicable law, with the possibility of an additional 45-day extension if necessary, in which case we will notify you of the reason for the extension.

14.3 Complaints and Regulatory Contacts

If you are not satisfied with our response to your privacy concerns, you may contact:

U.S. Securities and Exchange Commission (SEC)

Office of Investor Education and Advocacy

100 F Street, NE

Washington, DC 20549-0213

Telephone: 1-800-SEC-0330

Website: www.sec.gov

California Attorney General

Privacy Enforcement Section

1300 I Street

Sacramento, CA 95814

Telephone: (916) 210-6276

Website: oag.ca.gov/privacy

California Privacy Protection Agency (CPPA)

2101 Arena Boulevard

Sacramento, CA 95834

Email: regulations@cppa.ca.gov

Website: cppa.ca.gov

ADDITIONAL DISCLOSURES

State-Specific Provisions

Vermont Residents: Vermont law imposes additional restrictions on sharing information about Vermont residents. We will not share information we collect about you with nonaffiliated third parties unless authorized by you or as permitted by Vermont law.

Massachusetts Residents: If you are a Massachusetts resident, we will obtain your consent before sharing your personal financial information with nonaffiliated third parties, except as permitted by law.

Other States: We comply with applicable state privacy laws in all jurisdictions where we conduct business. If you reside in a state with specific privacy protections, those protections apply to you.

International Users

Our services are provided from the United States and are intended for users located in the United States. We do not market services to persons located outside the United States. If you access our website from outside the United

States, your information may be transferred to, stored, and processed in the United States. The United States may have data protection laws that are different from the laws of your country.

Recordkeeping and Retention Schedules

As a registered investment adviser, we are subject to recordkeeping requirements under SEC regulations. We maintain books and records in accordance with SEC Rule 204-2, which generally requires retention of records for at least six years after the end of the fiscal year in which the last entry was made. These records may include communications, account documents, advisory agreements, performance reports, and other information necessary for our regulatory compliance.

Automated Decision-Making

We may use automated systems and algorithms to assist in portfolio management, investment recommendations, and risk assessment. However, our investment advisers review and oversee automated recommendations to ensure they are appropriate for your individual circumstances. You may contact your advisor at any time to discuss our recommendations and the factors we consider.

Employee and Job Applicant Information

If you are an employee of Farther or have applied for employment, we collect and use your personal information for human resources, payroll, benefits administration, and other employment-related purposes. Employee information is subject to our internal employee privacy policies and applicable employment laws. California employees and job applicants have rights under the CCPA regarding their personal information.

DEFINITIONS

Affiliate: A company that controls, is controlled by, or is under common control with another company.

Consumer: Under the GLBA, an individual who obtains or has obtained a financial product or service from us for personal, family, or household purposes.

Customer: Under the GLBA, a consumer who has a continuing relationship with us, such as an ongoing investment advisory relationship.

Nonaffiliated Third Party: Any person or entity that is not an affiliate of Farther.

Nonpublic Personal Information (NPI): Personally identifiable financial information that is not publicly available, including information provided to us, resulting from transactions with us, or otherwise obtained by us in connection with providing financial services.

Personal Information: Under the CCPA, information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a particular consumer or household.

Prospective Client: An individual who has inquired about or is considering our services but has not yet entered into an investment advisory agreement with us.

Sensitive Customer Information: Under SEC Regulation S-P, any component of customer information, alone or in combination, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience, such as Social Security numbers, account numbers with security codes, biometric information, and health information.

Sensitive Personal Information: Under the CCPA, specific categories of personal information that present heightened privacy risks, including Social Security numbers, precise geolocation, racial or ethnic origin, religious beliefs, health information, sex life or sexual orientation, and biometric information.

ACKNOWLEDGMENT AND CONSENT

For Existing Clients: By entering into an investment advisory agreement with Farther Finance Advisors, you acknowledge that you have received, read, and understand this Privacy Policy and consent to the collection, use, and disclosure of your personal information as described herein and in accordance with applicable law.

For Prospective Clients and Website Visitors: By providing us with your personal information, using our website, or continuing to interact with us after receiving this Privacy Policy, you acknowledge and consent to the practices described in this Privacy Policy.

California Residents: If you are a California resident whose information is subject to the CCPA, this Privacy Policy serves as our notice at collection under the CCPA, informing you of the categories of personal information we collect, the purposes for which we use each category, and your rights regarding your information.

Thank you for entrusting Farther with your financial future. Protecting your privacy and security is fundamental to our relationship with you.