PRIVACY POLICY

Notice at Collection

Effective: October 2, 2025

ClairFi Technologies Inc., doing business as ClairFi ("**ClairFi**," "**we**," "**our**," or "**us**"), is collecting your PI ("**PI**") and, where necessary, certain categories of sensitive PI to provide and operate the ClairFi Services. ClairFi operates a technology platform and marketplace that connects users with independent third-party financial, tax, legal, and related professional service Providers (the "**Providers**"). ClairFi provides platform infrastructure (including a secure virtual vault and an AI-powered Research Bot), matching, subscription, and payment management, and administrative services to facilitate introductions and the delivery of platform features. ClairFi is a technology platform only and does not provide professional investment, tax, legal, or insurance advice; Providers are independent and are responsible for the professional services they provide and the PI they collect under separate engagement agreements. We collect information for the business purposes described below, including matching you to Providers, onboarding and identity verification (KYC/AML), subscription and payment processing, billing and refunds, facilitating Provider engagements, operating and securing the virtual vault and Research Bot, customer support, fraud prevention, product and service improvement (including analytics), and to comply with legal and regulatory obligations. We use Stripe Inc to process payments. Stripe may use your payment data in accordance with the terms of its privacy policy located at **https://stripe.com/privacy**.

ClairFi does not sell your PI and does not share PI for cross-context behavioral advertising. We do not currently engage in practices that constitute a "sale" or "sharing" of PI as those terms are defined under the CCPA/CPRA. If our practices change in a way that would constitute a sale or sharing under applicable law, we will provide advance notice and update this Notice and our Privacy Policy with opt-out instructions where required.

Our Privacy Policy and California Privacy Notice can be found at **https://clairfi.com/privacy/**.

We may collect the categories of PI and sensitive PI described in the tables below. For each category, we identify typical retention periods and our primary business purposes for collecting and using data (*e.g.*, Provider matching, subscription management, onboarding and compliance, billing and tax compliance, and providing virtual vault and Research Bot functionality). The tables summarize expected categories and retention; specific retention and use may vary by Service, Provider engagement, or applicable law.

PI Category	Retention Period	Business Purpose	Sold or Shared
Identifiers, including real name, alias, postal address, email address, telephone number, online identifiers, account name, Internet Protocol (IP) address, device identifiers, and government identifiers such as Social Security number, driver's license, or passport number when required for identity verification, onboarding, or tax/IRS compliance.[1]	Retained for the duration of your active account and for up to 5 years after account closing for business, compliance, audit, and dispute-resolution purposes, except where a longer statutory retention period applies.	Used for Provider matching and onboarding, identity verification and KYC/AML, account and subscription management, payment and billing, customer support, fraud detection and security, and to comply with legal and regulatory obligations. We use identifiers to operate and secure the virtual vault, as well as to facilitate Provider engagements with your instructions.	No. We do not sell or share these identifiers for cross-context behavioral advertising.
California customer records PI and financial information, including bank account and routing numbers, partial or masked card data (third-party PCI-compliant payment processors process full card numbers), tax documentation (*e.g.*, taxpayer ID numbers, tax returns, W-9s, and other tax filings), and financial records you upload to the virtual vault (including the ClairFi IRS vault for tax compliance and filing support). Some PI included in this category may overlap with other categories.	Retention varies by subcategory: identity and onboarding documents are retained for the active account period and up to 5 years after account closing for business and compliance purposes. Tax and IRS-related documents are stored in the ClairFi IRS vault and retained for up to 7 years to satisfy IRS and tax record retention obligations.	Used to facilitate tax filing and reporting with Providers, to perform KYC/AML and regulatory compliance checks, to process payments and refunds, to maintain billing and transaction histories, and to facilitate Provider services where necessary to deliver the requested professional services.	No. We do not sell or share this financial information for cross-context behavioral advertising.
Protected classification characteristics (*e.g.*, age, citizenship, gender, disability status, and other demographic profile information) to the extent you provide them or where they are necessary for a Service.	Retained for the duration of the account and up to 5 years after account closing, unless a different legal, contractual, or statutory retention requirement applies.	Used for Provider matching, personalization of Services, and as otherwise required or permitted by law.	No. We do not sell or share this category for cross-context behavioral advertising.

[1] Includes identifiers provided during Provider engagements or uploaded to the virtual vault.

PI Category	Retention Period	Business Purpose	Sold or Shared
Commercial information, including selected subscription plans, billing and transaction history, engagement letter status, invoices, and records of products or services purchased through the platform or from Providers.	Retained for the duration necessary to support billing, refunds, regulatory and tax compliance, and fraud prevention; up to 5 years after account closing for compliance and audit purposes, subject to applicable law.	Used for subscription and payment management, billing, refunds, payment reconciliation with Providers, tax and regulatory reporting, and fraud prevention.	No. We do not sell or share this category for cross-context behavioral advertising.
Biometric information (*e.g.*, fingerprints, faceprints, voiceprints, or other biometric templates): not collected for platform purposes as a routine matter. If we implement a narrow verification feature that requires biometric data, we will provide a separate notice and obtain your explicit consent where required by law.	If collected with explicit consent for a narrowly scoped verification purpose, retained only as necessary for that purpose and in accordance with applicable law, and any separate notice provided at the point of collection.	Used only for the stated verification purpose (*e.g.*, identity verification) and subject to enhanced protection.	No. We do not sell or share biometric information for cross-context behavioral advertising. If we do, we will narrowly scope any collection and will disclose it in a separate notice.
Internet or other similar network activity, including IP addresses, device and browser identifiers, operating system, usage and diagnostic data, log files, and Research Bot session inputs (*see the Research Bot entry below for session retention practices*). This category includes information collected automatically to operate, secure, and improve the Services.	Retained for operational, security, and analytics purposes for the duration necessary to provide the Services and for up to 5 years after account closing for logs, security investigations, and compliance, subject to specific vendor retention terms and legal obligations.	Used to operate, secure, and improve the Services (*including performance monitoring and analytics*), to detect and prevent fraud and abuse, and to support customer service and technical troubleshooting.	No. We do not sell or share this category for cross-context behavioral advertising.
Geolocation data: we may collect general location information (*e.g.*, city, state, or country). Precise geolocation data is not collected as a routine matter and will only be collected if you explicitly enable a location feature for a specific Service, in which case we will notify you at the point of collection.	If collected, retained only as necessary to provide the specific feature and in accordance with our general retention rules and any applicable legal requirements; otherwise, typical logs may be retained for up to 5 years as described above.	Used to improve matching, to provide localized features, and to support Services that require location information; precise location collection requires your consent and is limited to the specified purpose.	No. We do not sell or share geolocation data for cross-context behavioral advertising.

PI Category	Retention Period	Business Purpose	Sold or Shared
Sensory data, such as images, voice recordings, or videos, where you choose to provide such media for identification, onboarding, Provider interactions, or customer service. We collect such data only with notice and, where required, consent.	Retained only as necessary for the purpose for which it was collected (*e.g.*, onboarding or verification) and in accordance with our retention schedules; tied to the account lifecycle and up to 5 years after account closing for investigation and compliance purposes, unless law requires otherwise.	Used for identity verification, onboarding, Provider interactions, and customer support.	No. We will not sell or share sensory data for cross-context behavioral advertising unless there is a necessary legal basis and user consent is obtained where required.
Professional or employment-related information, such as your current or past job history, credentials, and professional background, that you provide to help match you with Providers.	Retained for the duration necessary to provide the Services and for up to 5 years after account closing, unless otherwise required by law or contract.	Used for Provider matching, personalization, and to facilitate the delivery of Services by Providers.	No. We do not sell or share this category for cross-context behavioral advertising.
ClairFi does not routinely collect non-public education information; we will only collect such information if you voluntarily provide it (*e.g.*, to support a Provider engagement). If provided, retention and use will follow the purposes and retention periods described elsewhere in this Notice.	Retained only as necessary for the purpose provided and for up to 5 years after account closing unless law requires otherwise.	Used to facilitate Provider services where relevant.	No. We do not sell or share this category for cross-context behavioral advertising.
Inferences drawn from other PI, such as profiles that reflect preferences, characteristics, or other inferred attributes, are used to facilitate Provider matching, personalization, and service improvements.	Retained as necessary for matching and service improvement; personal-identifiable inferences are retained no longer than necessary for the purpose, while aggregated or de-identified inferences may be retained longer or indefinitely for analytics.	Used to improve matching, personalization, and analytics.	No. We do not sell or share inferences for cross-context behavioral advertising.
Other PI, including subscription and transaction history, payment, and billing	Retention depends on the specific subcategory: subscription and	Used to operate your account and subscriptions, to process payments and	No. We do not sell or share this

PI Category	Retention Period	Business Purpose	Sold or Shared
information (processed by third-party PCI-compliant payment processors), documents and materials you upload to the virtual vault, and Research Bot outputs that you expressly elect to save to the vault.	billing records, retained for up to 5 years after account closing for business and regulatory purposes; tax and IRS vault records, up to 7 years; documents uploaded to the vault, retained in accordance with your account settings and our retention schedule; Research Bot session inputs, deleted at session end unless you elect to save outputs into the vault (*see Research Bot entry and Data Retention sections in the Privacy Policy*).	refunds, to provide secure storage and Provider access (as directed by you), to support Research Bot functionality, and to comply with legal obligations and security requirements.	category for cross-context behavioral advertising.

Sensitive PI is a subtype of PI consisting of specific information categories. At the same time, we collect information that falls within the sensitive PI categories listed in the table below (*e.g.*, government identifiers, tax identifiers, and certain financial account details), ClairFi limits collection and use of sensitive PI to what is necessary for onboarding, billing, tax and IRS compliance, KYC/AML checks, fraud prevention, and to facilitate Provider services (the CCPA/CPRA's Permitted SPI Purposes). California residents have the right to request that we limit the use and disclosure of their sensitive PI to Permitted SPI Purposes and to exercise other rights described in this Privacy Policy. We will not discriminate against consumers for exercising their rights to privacy.

Sensitive PI Category	Retention Period	Business Purpose	Sold or Shared
Government identifiers, such as your Social Security number (SSN), taxpayer identification number, driver's license, state identification card, or passport number, are collected where required for identity verification, KYC/AML, tax filing facilitation with Providers, or IRS compliance.	Retained only as necessary for the purposes collected and in accordance with applicable law. We retain identity and onboarding documents for the active account period and up to 5 years after account closing; government identifiers and tax documents stored in the ClairFi IRS vault are retained for up to 7 years to meet IRS and tax-record retention obligations, unless a different statutory period applies.	Used for identity verification, KYC/AML, tax filing, and reporting with Providers, and to comply with legal and regulatory obligations.	No. We do not sell or share government identifiers for cross-context behavioral advertising.
Complete account access credentials (*e.g.*, usernames combined with passwords or security codes) and authentication information. We securely store authentication credentials (hashed/encrypted) and use authentication tokens in accordance with secure authentication practices.	Retained only as necessary to support account authentication and security, for the duration of your account and as required to meet security and business needs; credentials are protected using appropriate encryption and security controls.	Used to authenticate you, to secure access to your account, and to support fraud prevention and account recovery.	We do not disclose credentials except as required by law or as necessary to provide Services under secure contracts.
Precise geolocation (*i.e.*, physical location within a small radius) is not routinely collected. It will only be collected if you enable a specific feature that requires precise location for a stated purpose.	Retained only as necessary to provide the requested feature and in accordance with applicable law and our retention rules. No sale or sharing for	Used only to provide the specific feature for which you enabled precise geolocation, and only with your consent.	No sale or sharing for cross-context behavioral advertising.

Sensitive PI Category	Retention Period	Business Purpose	Sold or Shared
	cross-context behavioral advertising.		
Racial or ethnic origin: collected only if you voluntarily provide it or where necessary for a Service (*e.g.*, voluntary demographic information used for matching).	Retained only as necessary and for up to 5 years after account closing.	Used where necessary for tax, onboarding, or Provider services.	No sale or sharing for cross-context behavioral advertising.
Citizenship or immigration information.	Retained only as necessary and in accordance with applicable law.	Used where essential for tax, onboarding, or Provider services.	No sale or sharing for cross-context behavioral advertising.

If you have any questions about this Notice or need to access it in an alternative format due to a disability, please contact **privacy@clairfi.com**. You may also contact us by mail at ClairFi Technologies Inc. (d/b/a ClairFi), Attn: Privacy Team, 26077 Nelson Way, Ste 502, Katy, TX 77494.

To exercise your privacy rights, including CCPA/CPRA or other state rights, you may (1) use the account self-service tools in the ClairFi portal (**https://www.clairfi.com/account**), (2) submit a request via email to **privacy@clairfi.com**, or (3) contact us by mail at the address above. We will verify your identity before responding to rights requests and will respond within the timeframes required by applicable law. (*See our California Privacy Notice within the Privacy Policy for California-resident-specific instructions and opt-out mechanisms.*)

Privacy Policy

Last updated: October 2, 2025.

NOTICE REGARDING SALE OR SHARING OF PERSONAL INFORMATION: ClairFi does not sell or share personal information for cross-context behavioral advertising. We do not share personal information in a manner that constitutes a "sale" or "sharing" under the CCPA/CPRA, nor do we process biometric data for platform purposes unless expressly disclosed, consented to, and required for specific service features. If our practices change (*e.g.*, we begin selling personal information or using biometric data), we will provide advance notice and update this policy and applicable California-specific notices.

ClairFi Technologies Inc., doing business as ClairFi ("**ClairFi**", "**we**", "**our**", or "**us**"), operates a technology platform that connects users with third-party financial, tax, legal, and related service providers (the "**Virtual Family Office**" or "**Providers**"). ClairFi provides the platform, tools (including a secure virtual vault and an AI-powered Research Bot), and administrative services necessary to facilitate introductions, matching, and the delivery of certain platform features. Third-party Providers are independent contractors or entities; they are responsible for the personal data they collect, process, and retain while providing professional services to you under separate engagement agreements. ClairFi's role is that of a technology platform and marketplace, not a provider of professional investment, tax, legal, or insurance services.

This policy applies to personal data we collect and process in connection with our provision of the ClairFi Services, including through our website, mobile applications, virtual vault, Research Bot, email communications, customer support, and other online features or tools that link to this policy (collectively, the "**Services**"), including via the following:

- Through the Services.
- In communications, including email, text, chat, and other electronic messages, between you and the Services or Providers accessed through the Services.
- When you interact with advertising, forms, or applications delivered through the Services or when interacting with Platform features that involve third-party Providers.

- Other sources where we have lawful grounds to process your personal data in connection with the Services.

This policy does not apply to: (a) information collected offline or through other websites or services that do not link to this policy; or (b) personal data collected, processed, or stored directly by third-party Providers in the Virtual Family Office or other third parties, who will have their own privacy notices and engagement agreements governing their data practices, including the following:

- Third parties (including Providers and other service partners) that collect or process personal data in connection with their own services and that do not operate under this privacy policy.
- Any third-party websites, applications, services, or content that you access from or through the Services; those entities are responsible for their own privacy practices.

We may provide additional or different privacy notices that are specific to certain Services, features, Providers, or transactions. Where a Provider or third-party provides a separate privacy notice in connection with a service, that notice governs the Provider's or third-party's processing of personal data in relation to that service.

Please read this policy carefully. By using or accessing our Services, or by providing personal data to ClairFi or to Providers through the Services, you agree to the collection, use, and disclosure of your personal data as described in this policy. We reserve the right to modify this policy at any time. Material changes will be posted with an updated "Last updated" date, and where required by law, we will provide notice by email or an in-service notice.

Children's and Minors' Data

The Services are intended for persons who are 18 years of age or older. We do not knowingly collect personal data from children under 13 and do not permit them to register for the Services. We comply with all requirements of the Children's Online Privacy Protection Act (COPPA). We implement reasonable measures to prevent the collection of data from children under 13. If we become aware that we have collected personal data from a child under 13 without verified parental consent, we will take steps to delete that information as required by law. For users who are minors under 18 but over 13, we do not permit registration; if an account created by or on behalf of a person under 18 is discovered, ClairFi will cancel the account and, where applicable under our Refund Policy, refund amounts paid for the subscription if no engagement letter has been executed and no investment activity has occurred.

The Personal Data That We Collect or Process

"**Personal data**" (or "**personal information**") means information that identifies, relates to, or is reasonably capable of being associated with an identifiable individual. For ClairFi, this commonly includes the following:

- Name
- email address
- telephone number

- postal address
- financial profile data
- financial data and statements
- tax documentation (including taxpayer identification numbers or Social Security numbers when required for regulatory or IRS compliance)
- bank or payment account details
- subscription and transaction history
- other identifiers or information necessary to provide matching, onboarding, compliance, and Services.

Certain categories, including tax identifiers, government ID numbers, and specific financial and health-related information, are considered sensitive and are subject to enhanced security and legal protections.

The types and categories of personal data we collect or process include, but are not limited to, the following:

- Account and contact information, including name, postal address, email address, phone number, username, and other contact details you provide when creating or updating an account.
- Payment and billing information, including credit/debit card information or other payment method details processed by our payment processors when you purchase a subscription or Services. Our credit card processing is handled by Stripe, Inc, a PCI DSS-compliant third-party payment processor that maintains appropriate security certifications and compliance programs. Stripe may use your payment data in accordance with its privacy policy, https://stripe.com/privacy.
- Account history and subscription data, including plan selected, billing history, transaction records, engagement letter status, and service usage records.
- Demographic information and profile data you elect to provide (*e.g.*, professional status, income range, tax filing status, city/state) used for matching and personalization; collection is limited to what is necessary and, where required, collected only with your consent.
- Location information (general geographic region such as country, state, or city). We do not collect precise geolocation unless you explicitly enable or consent to location collection for a specific Service feature.
- Device and technical information, including IP addresses, device and browser identifiers, operating system, preferred language, and usage and diagnostic data collected automatically to operate and improve the Services.
- Content that you create, upload, or store in connection with the Services, including documents uploaded to the virtual vault, messages to Providers, and any profile information or feedback you provide.
- Images, voice recordings, or videos if you choose to provide them for identification, onboarding, or Provider interactions; storage and processing of such media are subject to your consent and the specific Service feature's requirements.
- Identity and tax documentation (*e.g.*, government ID numbers, taxpayer identification, tax returns) when required for onboarding, regulatory KYC/AML checks, tax filing facilitation with Providers, or IRS compliance; we handle such information with

heightened security controls and retain such information only as required by law or our contractual obligations.
- We do not collect biometric information and other highly sensitive data as a routine matter. If we require such data collection for a specific Service, we will obtain your explicit consent and disclose processing details in a separate notice.
- Other information you voluntarily provide or that is reasonably necessary to provide the Services.

Third-party Providers may collect additional categories of personal data in connection with the services they provide to you, governed by their own notices and engagement agreements.

If you are a California resident, additional rights and disclosures are described in our California Privacy Notice.

Certain categories of personal data described above—such as tax identifiers, government identification numbers, and other sensitive categories—will be processed only when necessary for the Services, to comply with legal obligations, or with your explicit consent where required by law. If you choose not to provide required sensitive data, we may be unable to provide certain Services or complete certain transactions (*e.g.*, tax filing or onboarding with Providers).

We also collect:

- Statistics or aggregated information that does not directly identify you (*e.g.*, anonymized or aggregated usage metrics) derived from personal data and used for analytics, product improvement, and service development.
- Technical information and interaction logs, including clickstream data, pages visited, session times, and feature usage that help us maintain, secure, and improve the Services.

If we combine or connect non-personal statistical or technical data with personal data in a manner that identifies an individual, we treat that combined information as personal data and subject it to this policy.

How We Collect Your Personal and Other Data

You provide information to us when you register for or update your account, complete onboarding or Know Your Customer (KYC) procedures, upload documents to the virtual vault, interact with Providers, subscribe to or purchase Services, contact customer support, or otherwise communicate with us. You may also choose to submit content or feedback to the Services.

Information is also collected when you create or update a profile, request matching to Providers, consent to engage a Provider, use the Research Bot, or provide documents or materials to the virtual vault or to Providers. Some Provider engagements require direct sharing of your information with the Provider under a separate engagement agreement.

Automatically Through Our Services

As you navigate and use the Services, we collect certain information automatically for security, functionality, and analytics purposes. This may include usage details, IP address, device and browser type, operating system, and interaction data (*e.g.*, pages visited and session duration). ClairFi does not currently deploy advertising cookies or third-party tracking for behavioral advertising on its website; we do, however, collect standard technical telemetry and performance logs. We use Google Analytics, operating under our data processing agreement with Google, to collect standard website analytics data in compliance with applicable privacy laws.

We do not currently engage in cross-site behavioral advertising for profit. If that practice changes, we will update this policy and implement any required consent mechanisms in accordance with the relevant jurisdiction.

Automatic collection helps us provide and improve the Services, detect and prevent fraud or abuse, and maintain platform security and performance.

The automatic data collection technologies that may be used include cookies and web beacons. Currently, ClairFi does not use cookies for behavioral advertising or third-party ad targeting on the website. If this changes, we will provide a prominent notice and obtain any required consent.

- **Cookies.** Small files are placed on your device to support site functionality or analytics. You can disable cookies using your browser settings, but doing so may limit access to certain features. (If and when ClairFi implements cookies for additional purposes, we will disclose the types and provide consent controls.)
- **Web beacons**. Small files embedded in pages or emails to collect basic usage and deliverability information for system integrity and email analytics.
- **Other technologies**. We will use other technologies only as necessary for the Services (to be disclosed when implemented).

If we adopt additional automated technologies that create a legal obligation to provide opt-outs (including under the CCPA/CPRA's requirements regarding sales, sharing, and targeted advertising, or Nevada's requirements regarding sales of covered information), we will publish instructions and tools to facilitate the exercise of those opt-outs through clear and conspicuous mechanisms as required by applicable law. Please note that opting out of certain technologies may limit or disable some Services features. Users can submit opt-out requests through their account settings or by contacting privacy@clairfi.com.

Third parties that may use automatic collection technologies on or through the Services include analytics providers, infrastructure providers, email delivery services, and other service partners. We do not control the collection and use of such technologies by third parties; please contact the third party for more information about their practices.

- Analytics companies and other infrastructure providers used to operate or analyze the Services.
- Device manufacturers, internet service providers, and other third parties in connection with their own services and technologies.
- Other categories of third parties necessary to provide the Services (*e.g.*, payment processors, hosting providers, security vendors).

- Other categories of third parties as relevant to specific features.
- These third parties may use tracking technologies to collect information about your online activities and to provide targeted content or analytics. We do not control their tracking; please contact the third party for details about their use of tracking technologies and any available opt-out mechanisms.

We do not control third parties' tracking technologies or how they may be used. If you have questions about an advertisement or targeted content, you should contact the provider responsible for the advertisement or content.

We do not control the tracking technologies used by these third parties or how they may be used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

From business partners, third-party Providers, and service providers: We may receive personal data about you from Providers and third-party partners in connection with onboarding, KYC/AML checks, payments, or other services. Personal data provided by Providers is governed by the Provider's own privacy notices and the engagement agreement between you and the Provider.

Virtual Vault and Research Bot. ClairFi provides a secure virtual vault to store documents (including tax and financial records) and an AI-powered Research Bot for session-based analysis and research. Documents stored in the virtual vault are encrypted at rest and in transit, access-controlled, and retained in accordance with our retention policy (see Data Retention and Deletion). The virtual vault may store certain documents for compliance with IRS and business record retention obligations (see below). The Research Bot processes inputs on a session-by-session basis: uploaded data used solely for the Research Bot session does not persist as part of the Research Bot's model and is automatically deleted at the end of each session. Research Bot inputs are processed locally and are not transmitted to public internet search engines or third-party services without your explicit consent. We strongly discourage you from uploading unnecessary sensitive personal data (*e.g.,* full Social Security numbers) into the Research Bot; if you do upload sensitive data, it will be treated as described in this policy and protected with encryption and access-control measures.

How We Use Your Personal Data. We use personal data for the following purposes: to provide, operate, and improve the Services; to match you with Providers and facilitate Provider engagements; to administer accounts, billing, and subscriptions; to perform identity verification, KYC/AML, and fraud prevention; to comply with legal obligations and respond to legal requests; to communicate with you about your account, Service changes, and support; to power the Research Bot and platform analytics (subject to session-based deletion rules); and, with your consent where required, to send promotional communications. We rely on a variety of legal bases to process personal data, including contract performance, legal compliance, legitimate interests (such as fraud prevention and service improvement), and consent where required by law.

Sharing and Disclosure of Personal Data. We may share personal data with: (a) Providers you select or are matched with to enable the Provider to provide professional services to you under a

separate engagement agreement; (b) service providers and sub processors (such as hosting providers, payment processors, analytics vendors, identity verification vendors, and email delivery services) who perform services on our behalf under confidentiality and data protection obligations; (c) affiliates, in the event of corporate restructuring, merger, acquisition, or sale of assets (with notice where required by law); and (d) law enforcement, regulators, or other parties when required by law or to protect the rights, safety, or property of ClairFi, our users, or the public. Providers are independent and may be controllers of personal data they collect directly from you; ClairFi is not responsible for Provider privacy practices except as set forth in any engagement agreement or as otherwise required by law.

Data Transfers. ClairFi stores and processes data in the United States. We do not transfer personal data outside the U.S.; if we do so in the future, we will implement appropriate safeguards (*e.g.*, standard contractual clauses, adequacy decisions, or other transfer mechanisms) as required by applicable law. We will disclose those safeguards in this policy.

Data Retention and Deletion. We retain personal data only for as long as necessary to provide the Services, to comply with applicable laws and regulations, and to resolve disputes. Typical retention periods include the following:

- account and subscription records: retained for up to 5 years after account termination for business and compliance purposes;
- tax and financial records stored in the IRS vault: retained for up to 7 years to satisfy IRS and tax-record retention obligations;
- transaction records and billing: retained for regulatory and tax compliance as required;
- Research Bot session inputs: not stored persistently and deleted at session end (unless you expressly elect to save session outputs into the vault); and
- aggregated or anonymized data: retained as needed for business analytics. Upon deletion or account termination, we will delete or de-identify personal data as required by law, except for certain records we must retain to comply with legal obligations or legitimate business interests.

Security Measures. ClairFi implements industry-standard technical, administrative, and organizational measures to protect personal data, including encryption in transit (TLS) and at rest for sensitive data, access controls and role-based permissions, secure logging and monitoring, regular vulnerability assessments and patching, employee training, and use of reputable cloud and security vendors. In the event of a security incident involving personal data, we will follow our incident response procedures and provide notice to affected users and regulators without unreasonable delay and in accordance with all applicable state and federal laws, including but not limited to the Texas Identity Theft Enforcement and Protection Act.

Cookies and Tracking. ClairFi does not currently use cookies, pixels, or similar technologies for third-party behavioral advertising. We may use limited first-party cookies or analytics tools to enhance site functionality, security, and performance. Any use of persistent or third-party tracking for advertising or profiling purposes will be disclosed in an updated policy. Where required by law, we will obtain your consent and provide opt-out mechanisms.

Your Rights and Choices. Depending on your jurisdiction, you may have rights regarding your personal data, including: the right to access and obtain a copy of your personal data; the right to correct or update inaccurate data; the right to request deletion or restriction of processing; the right to portability; the right to object to certain processing or to opt out of targeted advertising and sale/sharing of personal information; and the right to withdraw consent where processing is based on consent. California residents have additional rights under CCPA/CPRA. To exercise these rights, you may: (a) use the account self-service tools in the ClairFi portal; (b) submit a request via **privacy@clairfi.com**; or (c) contact us by mail at ClairFi Technologies Inc., 26077 Nelson Way, Ste 502, Katy, TX 77494, Attn: Privacy. We will verify your identity before responding and will respond to requests within the timeframes required by applicable law (*e.g.*, within 45 days under the GDPR/CCPA, unless an extension is permitted).

Subscription, Payments, Refunds, and Account Deletion. ClairFi operates on a subscription model. Subscription fees and any additional fees for Provider services are described at the point of sale. Third-party, PCI-compliant payment processors process payments. Refunds are available only in accordance with ClairFi's Refund Policy, which is incorporated herein by reference. Specifically, a full subscription refund will be issued only where (a) no engagement letter has been executed with any Provider in the Virtual Family Office and (b) no investment or other billable activity has occurred through the platform; initial consultations with Providers do not disqualify a refund. Once an engagement letter has been executed or an investment has been made, the subscription is non-refundable. You may cancel your subscription at any time; cancellation will prevent further recurring charges but will not necessarily delete all account data immediately; retained data will be handled in accordance with our Data Retention and Deletion policy and applicable law.

Disclaimers and Limits on ClairFi Liability. ClairFi is a technology platform and does not provide professional investment, tax, legal, or insurance advice. Providers accessed through the platform are independent and responsible for their professional advice and services; you should review and rely on the Provider's engagement agreement and privacy notice for any professional services and data practices. Research Bot outputs are informational only and do not constitute professional advice; they should not be relied upon as a substitute for guidance from qualified Providers. To the maximum extent permitted by law, ClairFi expressly disclaims all liability for the services of Providers, advice from Providers, investment outcomes, or any decisions made in reliance on Research Bot outputs, and you acknowledge and agree to this disclaimer.

Third-Party Links and Third-Party Providers. The Services may contain links to third-party websites or resources and may facilitate direct interactions with third-party providers. We are not responsible for the privacy practices or content of those third parties. Before engaging a Provider, you should review the Provider's engagement agreement and privacy notice to understand how the Provider will use and protect your data.

Complaints and Dispute Resolution. If you have a privacy concern or complaint, please contact us first at **privacy@clairfi.com** or via mail at the address above. We will investigate and respond promptly. If you are not satisfied, you may have the right to lodge a complaint with the California Privacy Protection Agency or California Attorney General (for California residents), the Nevada Attorney General (for Nevada residents), or other applicable regulators. For disputes

related to this Privacy Policy, the dispute resolution provisions in our Terms of Use shall apply, including any applicable arbitration requirements, except where prohibited by law.

Changes to this Privacy Policy. We reserve the right to update this policy to reflect changes in our practices, legal obligations, or Services. When we make material changes, we will update the 'Last updated' date and provide additional notice as required by law. Continued use of the Services after changes are posted constitutes acceptance of the revised policy.

Contact Information. Questions, requests, or concerns about this Privacy Policy or ClairFi's data practices may be addressed to: **privacy@clairfi.com** or by mail at ClairFi Technologies Inc., 26077 Nelson Way, Ste 502, Katy, TX 77494, Attn: Privacy. ClairFi has designated our Privacy Team to handle data protection matters. For privacy-related inquiries, please contact privacy@clairfi.com.

We may receive personal data about you from other sources and combine that with information we collect directly from you. For example, we may obtain information about you from service providers that we engage to perform services on our behalf, such as email platform providers, content delivery network providers, payment processors, promotions and analytics providers, security and anti-fraud services, and data brokers. We may also receive personal data from business partners and third-party providers in the ClairFi Virtual Family Office (*e.g.*, accountants, tax preparers, RIAs, attorneys, insurance agents, and other professionals). Those third-party providers are independent entities that determine their own data -processing practices and are responsible for compliance with their own privacy and data-protection obligations under the engagement agreements you enter directly with them; ClairFi is not responsible for those third-party providers' privacy practices or for personal data they collect, process, or store pursuant to their separate agreements with you. We may combine information we receive from these sources with other information we have about you to provide, personalize, and improve our Services.

How We Use Your Information

We use information that we collect about you or that you provide to us, including any personal data, to support and operate our platform and Services, including to match you with third-party providers in the ClairFi Virtual Family Office, operate and secure your account and our secure virtual vault, and process interactions with the Research Bot and other automated features.

- Provide you with the Services and any contents, features, information, products, or services that we make available through the Services.
- Fulfill and manage subscriptions, payments, billing, provider engagements (including any engagement letters with Virtual Family Office providers), and refunds in accordance with our Refund Policy and applicable agreements.
- Fulfill any other purpose for which you provide it.
- Provide you with notices about your account and subscription, including expiration, renewal, billing, payment issues, and other account communications.
- Improve our Services, including by analyzing your information and creating aggregated or de-identified data to develop, maintain, analyze, improve, optimize, measure, and report on our Services and their features and how users interact with them. Our analysis

may utilize machine learning and other automated tools. We do not use personal data that you upload to the Research Bot to train models; Research Bot session data is deleted at the end of each session unless you explicitly save content to your secure virtual vault.
- Promote our Services, business, and offerings by sending you information about new features, offers, and services, and by personalizing content and communications. We may use information to model, segment, target, offer, market, and advertise our Services, subject to your choices, applicable legal requirements, and opt-out preferences.

Carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including those related to billing and collection.

- Notify you when service updates are available and about changes to any products or services we offer or provide through them.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

The usage information we collect, whether connected to your personal data or not, helps us improve our Services and deliver a better and more personalized experience by enabling us to:

- Estimate our audience sizes and usage patterns.
- Store information about your preferences, allowing us to customize the Services according to your individual needs and interests.
- Speed up your searches.
- Recognize you when you return to our Services.

We may also use your information to contact you about goods and services that may be of interest to you, including services offered by third-party providers accessible through the ClairFi platform. If you do not want us to use your information in this way, you may opt out by adjusting your marketing preferences in your account settings or by emailing **privacy@clairfi.com**.

We use location information to prevent fraud and abuse, enforce platform security, match you with appropriately located third-party providers, and comply with applicable legal or regulatory requirements.

Who We Disclose Your Information To

We may disclose aggregated information about our users, as well as information that does not identify any individual and cannot reasonably be used to identify an individual, without restriction.

We may also disclose personal data that we collect or you provide as described in this privacy policy:

- To our subsidiaries and affiliates, and to third-party providers in the ClairFi Virtual Family Office who provide services directly to you under separate engagement or service agreements.

- To contractors, service providers, and other third parties we use to support our organization (*e.g.*, hosting providers, payment processors, identity verification and KYC providers, analytics providers, customer support vendors, and security and anti-fraud vendors). These parties are contractually obliged to keep personal data confidential and to use it only for the purposes for which we disclose it to them.
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of ClairFi Technologies Inc.'s assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which ClairFi Technologies Inc. holds personal data, is among the assets transferred.
- To third parties to market their products or services to you only if you have affirmatively consented or opted in to those disclosures. Where applicable, we contractually require these third parties to maintain the confidentiality of personal data and use it only for the disclosed purpose. For more information, see our Marketing Preferences in your account settings.
- To fulfill the purpose for which you provide it. For example, if you give us an email address to use the "email a friend" feature of our Services, we will transmit the contents of that email and your email address to the recipient(s).
- For any other purpose disclosed by us when you provide the information.
- With your consent.

We may also disclose your personal data:

- To comply with any court order, law or regulation, or legal process, including to respond to any government, regulatory, or law-enforcement request (*e.g.*, KYC/AML inquiries, tax reporting obligations, and IRS or other regulatory requests), and to meet our legal and regulatory obligations.
- To enforce or apply our Terms of Use (see the Terms of Use posted on the Website) and other agreements, including for billing and collection purposes.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our organization, our customers, or others, including exchanging information with other companies and organizations for fraud protection and credit risk reduction.

The categories of personal data we may disclose include:

- Account and contact information (*e.g.*, name, email address, mailing address, and telephone number).
- Payment and billing information (*e.g.*, payment card details, ACH or bank account information processed by third-party payment processors, and other payment verification data). Sensitive financial information (such as partial account numbers or tax identifiers) may be stored in the secure virtual vault; Social Security numbers (SSNs) and full bank account numbers are subject to enhanced security controls and encryption when stored, and access is strictly limited to authorized personnel on a need-to-know basis in accordance with applicable law.
- Account history, including information about your subscription, account transactions, engagement letters, provider interactions, order history, and billing history.

- Demographic information (*e.g.*, age range, gender, income range, and other information you provide to help match you to providers).
- Location information, including general geographic location and, if you permit, more precise geolocation.
- Device information (*e.g.*, device identifiers, operating system, browser type, and IP address).
- Content and information you elect to provide to us, including documents and materials you upload to the virtual vault or submit to the Research Bot or to third-party providers through the platform.
- Images, voice recordings, and videos collected or stored in connection with the Services, if you choose to provide or upload such information.
- Identity document information (*e.g.*, driver's license or passport information) when provided for identity verification or KYC purposes.
- Biometric information is only collected if you provide it for identity verification or similar purposes and to the extent permitted by applicable law; such information will be collected and used only for the stated verification purpose and in accordance with legal requirements.
- Other information collected and described at the point of collection.

Your Rights and Choices About Your Information

This section describes mechanisms you can use to control certain uses and disclosures of your information and rights you may have under state, federal, and international law, depending on where you live.

Advertising, marketing, cookies, and other tracking technologies choices:

- **Cookies and Other Tracking Technologies**. We do not currently use cookies, pixels, or similar tracking technologies for advertising or analytics on the Website. If ClairFi adopts cookies, pixels, or other tracking technologies in the future, we will provide advance notice, update this policy, and implement any required consent or opt-out mechanisms in accordance with applicable law. You may still set your browser to refuse cookies, but certain features may not function if and when we later implement cookie-based features.
- **Promotions by ClairFi**. If you do not wish us to use your information to promote our own or third parties' products or services, you can opt out by adjusting your account settings or by emailing **privacy@clairfi.com**. You may also unsubscribe from promotional emails using the unsubscribe link included in the communications.
- **Targeted Advertising by ClairFi**. We do not currently engage in targeted advertising using data sold or shared with unaffiliated third parties. If we change this practice, we will notify users and provide required opt-out mechanisms in accordance with applicable law.
- **Disclosure of Your Information for Third-Party Advertising**. We do not share personal data with unaffiliated third parties for interest-based advertising, except where you have provided affirmative consent to such sharing. We do not control the collection or use of information by third parties once they have received it directly from you.

Location data choices. You can choose whether to allow the Services to collect and use real-time information about your device's location through your device's privacy settings. If you block the use of location information, some Services features (including provider matching or localized offerings) may become inaccessible or not function properly.

Your State Privacy Rights

Subject to applicable state law and any relevant exceptions or limitations, you may have certain rights related to your personal data, including:

- **Access and Data Portability.** You may confirm whether we process your personal data and request access to a copy of the personal data we process about you. To the extent required by applicable law (*e.g.*, CCPA/CPRA or GDPR), we will provide requested data in a portable and, where feasible, machine-readable format and may provide additional information required by law.
- **Correction**. You may request that we correct inaccuracies in your personal data that we maintain, considering the nature of the information and the purpose for which it is processed.
- **Deletion**. You may request that we delete personal data about you that we maintain, subject to exceptions under applicable law (*e.g.*, where retention is necessary to comply with legal or regulatory obligations, to complete a transaction you requested, to detect or prevent fraud, to exercise or defend legal claims, or to comply with IRS and tax-record retention requirements). To submit a deletion request, you may email **privacy@clairfi.com** with the subject line "*Privacy Deletion Request*." We will verify your identity as reasonably necessary before fulfilling a deletion request and will respond within the timeframes required by applicable law. If we decline a request in whole or in part, we will provide the reason for the refusal. We will verify deletion requests through a two-step verification process and respond within 45 calendar days, with a possible 45-day extension if reasonably necessary.
- **Opt Out of Targeted Advertising, Profiling, and Sales**. You may request that ClairFi not use your personal data for targeted advertising, automated profiling that produces legal or similarly significant effects, or for any disclosures that constitute a "sale" or "sharing" under applicable privacy laws. ClairFi does not currently sell personal data as defined in the CCPA/CPRA and related statutes; nonetheless, we will honor verifiable opt-out requests where required by law. To opt out, use your account settings or submit a request to **privacy@clairfi.com**. Certain processing, such as matching you to third-party providers, performing compliance checks, or operating the Research Bot and the virtual vault to provide the Services, may involve profiling or automated processing necessary to provide the service and may therefore be subject to statutory exceptions.

Important: The exact scope of these rights varies by jurisdiction. Applicable law may limit or qualify our obligations to delete, disclose, or restrict processing of personal data (*e.g.*, to permit continued retention where necessary to provide the Services you requested, for tax or IRS compliance, to comply with legal process, or to detect or prevent fraud). Where an exception applies, we will notify you of the reason for any denial to the extent required by law.

To exercise any of these rights, you may submit a request by emailing **privacy@clairfi.com** with the subject line indicating the request type (*e.g.*, "Access Request," "Deletion Request," "Opt-Out Request"). We will require reasonable information to verify your identity before fulfilling requests. We will acknowledge receipt and respond within the applicable statutory timeframe (*e.g.*, we generally aim to respond within 45 days where required by law; shorter timelines may apply under other laws). To appeal a decision regarding a consumer rights request, email **privacy@clairfi.com** with the subject line "Privacy Appeal." Our Privacy Team will review appeals and provide a written response. If you remain unsatisfied, you may escalate the matter to the supervisory authority for your jurisdiction (*e.g.*, the California Attorney General for certain California residents).

Some browsers and browser extensions support the Global Privacy Control ("**GPC**"), which allows you to send a signal indicating your choice to opt out of certain types of data processing, including data "sales" as defined under specific laws. If technically feasible and required by applicable law, when we detect and can verify a valid GPC signal, we will process such signals as opt-out requests to the extent mandated by applicable law, subject to technical limitations and legal exceptions. You can also exercise these choices via your ClairFi account settings or by contacting **privacy@clairfi.com**.

Nevada Residents. Nevada provides its residents with a limited right to opt out of the sale of certain types of personal data. ClairFi does not currently sell personal data that would trigger Nevada's opt-out requirements. Nevada residents who wish to submit a request regarding data sales or to confirm our practices may contact us by e-mailing us at privacy@clairfi.com.

California Residents. If you are a California resident, additional rights and disclosures may apply under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). For a supplemental California privacy notice describing your rights and ClairFi's disclosures under California law, reference this Privacy Policy.

How We Protect Your Personal Data

We use commercially reasonable administrative, physical, and technical measures designed to protect your personal data from accidental loss or destruction and from unauthorized access, use, alteration, and disclosure. These measures include industry-standard encryption for data in transit (TLS 1.2 or higher) and encryption at rest (AES-256 for all stored personal and financial data) (*e.g.*, AES-256 for stored data where used), role-based access controls, multi-factor authentication for privileged access, regular vulnerability scanning and penetration testing, logging and monitoring, and periodic third-party security assessments and audits. Personal data stored in the ClairFi virtual vault is protected with enhanced access controls and encryption, and is accessible only to you and those you authorize, or as otherwise required by law. Data submitted to the ClairFi Research Bot is processed in isolated sessions and deleted at the end of each session, except as required for troubleshooting or to fulfill legal obligations (see the Research Bot section of this policy). We also require contractual and security commitments from third-party service providers that process personal data on our behalf. Despite these measures, no system is completely secure; we cannot guarantee absolute security. In the event of a security incident, we will comply with all applicable breach notification laws and notify affected individuals and regulators as required by law. In the event of a security incident affecting

personal data, we will notify the affected individuals without unreasonable delay and as soon as reasonably practicable and without unreasonable delay following discovery, 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, and will notify the relevant regulators as required by applicable law. We maintain SOC 2 Type II certification and conduct annual third-party security audits.

The safety and security of your information also depend on you. You are responsible for maintaining the confidentiality of your account credentials, choosing a strong password, enabling multi-factor authentication where available, and promptly notifying us of any unauthorized access or suspected account compromise. You should not share account credentials. You should also avoid uploading highly sensitive personal information (*e.g.*, full Social Security numbers, tax ID numbers, bank account passwords, or security credentials) into the Research Bot or in non-vault areas of the platform; if you choose to provide such information despite this warning, you do so at your own risk, acknowledge the inherent risks of transmitting such sensitive information, and expressly consent to the processing described in this policy.

How We Retain Your Personal Data

We retain the categories of personal data described in this policy for as long as necessary to provide the Services, to fulfill the purposes described in this policy, and to meet legal, tax (including IRS), and compliance obligations. In general: (a) account and profile information is retained for the duration of your active subscription and for a period of up to 5 years after account termination to support audits, resolve disputes, and maintain business records; (b) financial, tax, and filings information placed in the ClairFi IRS vault is retained for 7 years from the date of filing or last account activity (whichever is later) to support IRS and tax compliance, unless a different statutory period applies; (c) data uploaded to the Research Bot is processed on a session-by-session basis and is automatically deleted at the end of each session except where temporarily retained for technical troubleshooting purposes (not to exceed 30 days) or as required by applicable law; and (d) aggregated or de-identified data may be retained indefinitely. We may retain personal data for longer periods when necessary to comply with legal obligations, to establish or defend legal claims, or for legitimate business purposes. In such cases, we will notify you as applicable.

If you are a California resident and have specific questions about retention periods that apply to your personal data or wish the retention periods described in the section above apply to all personal information we collect, including information collected from California residents orto request deletion under California law, please contact **privacy@clairfi.com** with subject line "California Privacy Request".

Changes to Our Privacy Policy

We reserve the right to update this policy from time to time. The date this privacy policy was last updated is identified at the top of the page. For material changes that affect how we process your personal data or that reduce your rights, we will provide at least 30 days' advance notice to affected users (*e.g.*, by a prominent notice on the Services and via email to the address associated with your account). We will provide you with the opportunity to review the changes before they

take effect, where required by applicable law. For non-material changes, we will update the policy and post the revised policy on the Services. You should review this policy periodically.

Contact Information

To exercise your rights, to ask questions about this privacy policy, or to contact us about our privacy practices, please contact ClairFi Technologies Inc. via e-mail at **privacy@clairfi.com** or via regular postal mail at the following mailing address:

ClairFi Technologies Inc.
Attn: Privacy Team
26077 Nelson Way, Suite 502
Katy, TX 77494

For privacy requests and inquiries, please contact us by email at privacy@clairfi.com. Additional contact methods may be available based on your jurisdiction and the nature of your request.

To register a complaint or concern, please submit a detailed description of your issue to **privacy@clairfi.com**. We will acknowledge receipt and attempt to resolve the complaint. If you are a California resident and your complaint remains unresolved after 45 days, you may contact the California Attorney General's office. Nothing in this policy limits your right to file a complaint with relevant regulatory authorities. For other jurisdictions, we will provide contact information for the appropriate supervisory authority upon request.

Mobile App Privacy Policy

Introduction

ClairFi Technologies Inc., doing business as ClairFi ("**ClairFi**", "**we**", or "**us**"), respects your privacy and is committed to protecting it through our compliance with this policy. This policy describes:

- The types of information we may collect or that you may provide when you download, install, create an account for, access, or use the ClairFi mobile application and related services (the "**App**" or the "**Services**"), including information provided to or captured by the secure virtual vault and the AI-powered Research Bot.
- Our practices for collecting, using, maintaining, protecting, retaining, and disclosing that information and how you can exercise your privacy rights under applicable laws *(e.g.,* CCPA/CPRA, GDPR, and COPPA where applicable).

This policy applies to personal data we collect and process in connection with our provision of the App and the ClairFi Services, including through the App, the secure virtual vault, the Research Bot, in-app messages, email, text, customer support communications, and other online features or tools that link to this policy (collectively, the "**Services**").

This policy DOES NOT apply to information that: (a) is collected offline or through other websites or services that do not link to this policy; or (b) is collected, processed, or stored

directly by independent third-party Providers in the ClairFi Virtual Family Office or other third parties, who will have their own privacy notices and engagement agreements governing their data practices. Where a third-party Provider has its own privacy notice, that notice governs the Provider's processing of your data in connection with the Provider's services.

- We do not control the privacy practices of third parties, including Providers, and encourage you to review any third party's privacy notice before providing personal information to them.
- Information you provide to, or that we collect, other apps, websites, or content that may link to or be accessible from or through this App (*see "*Third-party Information Collection" and Provider-specific notices).
- Our websites, the App, and other third parties may have their own privacy policies, which we encourage you to read before providing information on or through them.

Please read this policy carefully to understand our policies and practices regarding your information and how we will treat it. If you disagree with our policies and practices, do not download, create an account, or use this App. By downloading, creating an account, or using this App, you expressly consent to and agree to be bound by this privacy policy. We reserve the right to update this policy from time to time in our sole discretion. Material changes will be posted with an updated "Last modified" date, and where required by law, we will provide notice by email and a prominent in-app notice at least 30 days before such changes take effect. Upon request, we will provide a copy of past material changes in a format that is accessible. Continued use of the App after revisions constitutes acceptance of the revised policy.

This policy is subject to change from time to time (*see* Changes to Our Privacy Policy). Your continued use of this App after we revise this policy indicates your acceptance of those changes. Please check the policy periodically for updates.

Children and Minors

The Services are intended for persons who are 18 years of age or older. We do not knowingly collect personal data from children under 13 and do not permit them to register for the Services. We comply with all requirements of the Children's Online Privacy Protection Act (COPPA). We implement reasonable measures to prevent the collection of data from children under the age of 13. If we become aware that we have collected personal data from a child under 13 without verified parental consent, we will take steps to delete that information as required by law. For users who are minors under 18 but over 13, we do not permit registration; if an account created by or on behalf of a person under 18 is discovered, ClairFi will cancel the account and, where applicable under our Refund Policy, refund amounts paid for the subscription if no engagement letter has been executed and no investment activity has occurred.

Information We Collect and How We Collect It

We collect information from and about users of our App from the following sources and process it on lawful bases appropriate to the jurisdiction *(e.g.,* contract performance, legal compliance, legitimate interests, and consent where required):

- Directly from you when you provide it to us *(e.g.,* during account creation, onboarding, or Provider engagements).
- Automatically when you use the App *(e.g.,* device and usage data, diagnostic logs, and Research Bot session telemetry).
- From third parties and Providers *(e.g.,* service providers, payment processors, identity-verification vendors, and Providers in the Virtual Family Office) and from publicly available sources or business partners.

Information You Provide to Us

When you download, create an account, or use this App, you may provide information about yourself, which may include (where applicable and necessary for the Service): your name, contact details (email address, telephone number, postal address), login credentials, date of birth (to verify age), financial profile data *(e.g.,* income range, net worth, accreditation status), tax documentation and taxpayer identification numbers (including Social Security numbers or other government tax identifiers when required for IRS or tax-filing purposes), identity documents (for KYC/AML onboarding), payment and billing information, subscription and transaction history, documents you upload to the virtual vault *(e.g.,* tax returns or financial statements), and any other information you provide when interacting with Providers or using the Services.

- Examples of personal information and sensitive personal information we may collect directly from you include: identifiers (name, email, postal address, device identifiers); financial information (income range, bank account/ACH details, transaction and subscription history); government and tax identifiers (SSN, taxpayer ID); identity documents (driver's license, passport); account and usage data; demographic information; and documents uploaded to the virtual vault (which may include financial, tax, and other sensitive documents).
- Information that is about you but does not, on its own, identify you *(e.g.,* aggregated or de-identified usage metrics), which we may combine with other data to provide and improve the Services.

This information includes data you provide by filling in forms in the App (for account creation, onboarding, or Provider requests), content you upload to the virtual vault, Research Bot inputs and any outputs you elect to save, correspondence with ClairFi or Providers, survey responses, documents and records relating to Provider engagements, and transaction records for payments and refunds. We treat certain categories *(e.g.,* tax identifiers, government IDs, and documents containing financial or health-related details) as sensitive personal information and are subject to enhanced security and restricted processing.

- Information you provide by filling in forms in the App, including identity, onboarding, and KYC/AML disclosures required to match you with Providers or to enable tax-related services.
- Records and copies of your correspondence (including email, in-app messages, and phone numbers), including communications with Providers or ClairFi customer support.
- Your responses to surveys or other feedback tools we provide to improve matching and Services.

- Details of subscription, billing, purchases, and other transactions you carry out through the App. A PCI-DSS compliant third-party payment processor performs payment processing on our behalf; we do not store full credit card numbers or other payment card data in our systems. Payment information is collected and processed directly by our payment processor Stripe Inc, subject to their security policies and procedures.in our systems.
- Search queries, Research Bot session inputs (processed on a session basis and deleted at session end unless you elect to save outputs to the vault), and other content you submit to the App.
- Other information you voluntarily provide that is necessary to provide the Services or to meet legal and compliance obligations.

You may provide information for publication or display ("**Posted**") in public areas of the App or in communications with Providers ("**User Contributions**"). Your User Contributions are posted and transmitted to others at your own risk. They may be accessible to Providers and third parties in accordance with your account and Provider engagement settings. Use caution when posting or sharing personal information in these contexts.

Information We Collect Through Automatic Data Collection Technologies

As you navigate through and interact with our App, we may use automatic data collection technologies to collect certain information about your device and your browsing and usage activity and patterns for the purposes of operating, securing, and improving the Services, preventing fraud, and supporting Research Bot session processing.

- **Usage details and analytics, including access times, session duration, feature usage, error** logs, and other diagnostic data used to operate and improve the App and to detect and prevent abuse or fraud.
- **Device and technical information, including unique device identifiers, mobile advertising identifiers (where applicable)**, IP addresses, operating system, app version, browser type (if applicable), and mobile network information.
- **Stored information and files metadata when you permit the App to access device content *(e.g.,* photographs or other files you choose to upload). Data you upload to the virtual vault is encrypted in transit and at rest and access-controlled; see the Virtual Vault and Research Bot sections for additional details**.
- **Location information.** We do not routinely collect precise geolocation *(e.g.,* GPS-level data). We may collect general location information (such as city or state) or precise location only if you explicitly enable a specific feature that requires it, and we will disclose that at the point(s) of collection.

If you do not want us to collect certain automatic or location information, you may disable location services or delete the App from your device. Please note that some App features may be unavailable if location collection or automatic data collection is disabled. For choices regarding device-level identifiers and tracking, use your device's settings and App Privacy settings, where available.

As of the date of this policy, we do not sell or share personal information for cross-context behavioral advertising as defined under applicable privacy laws, including but not limited to the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA") or the Nevada Privacy of Information Collected on the Internet from Consumers Act ("Nevada Privacy Law"). We do not currently engage in cross-site or cross-context behavioral advertising for profit. If our practices change *(e.g.,* if we begin to sell or share data as defined by applicable law), we will provide advance notice, update this policy and any required California-specific notices, and implement opt-out mechanisms and consent where required by law.

The automatic data collection technologies that may be used include cookies (or mobile cookies), web beacons, SDKs, and similar technologies. Currently, ClairFi does not use persistent third-party cookies for behavioral advertising. We may use first-party cookies or analytics SDKs solely to support app functionality, security, and performance. If we adopt additional persistent tracking or advertising technologies, we will update this policy and provide required notices and opt-out mechanisms.

- **Cookies (or mobile cookies) and first-party analytics: used,** if at all, to support functionality, security, and performance. You can refuse cookies by changing device/browser settings, but some features may be limited.
- **Web beacons and pixels: used for system integrity and email deliverability analytics where applicable; not currently used for third-party** behavioral advertising by ClairFi.
- Other technologies as necessary to operate the Services; we will disclose their use and provide appropriate choices when implemented.

We may tie non-personal information collected automatically to personal information you provide to us to operate and improve the App, to prevent fraud, and to secure the Services. We do so only to the extent necessary and consistent with applicable law.

Third-party Information Collection

When you use the App or its content, certain third parties may collect information about you or your device. These third parties include (without limitation) Providers in the ClairFi Virtual Family Office (accountants, tax preparers, RIAs, attorneys, insurance agents, and other professionals), payment processors, hosting and infrastructure providers, analytics and error monitoring vendors, identity-verification providers, and other service partners. Providers are independent entities responsible for their own processing of data collected while providing professional services to you; before engaging a Provider, you should review the Provider's engagement agreement and privacy notice.

- Examples of third parties that may use automatic information collection technologies on or through the App include infrastructure and analytics providers, payment processors, identity-verification vendors, email delivery services, and other service partners.
- Analytics and performance vendors used to operate or analyze the Services.
- Your mobile device manufacturer and operating system providers, when relevant to device features and updates.

- Your mobile service provider and other technical service providers are used to deliver the App.
- Other third parties as required for specific App features or Provider services.

These third parties may use tracking technologies to collect information about you. ClairFi does not control the tracking technologies or practices of these third parties; please contact the third party directly for information about their data practices and opt-out options.

We do not control the collection and use of such technologies by third parties. If you have questions about an advertisement or targeted content, please contact the provider responsible for that content directly. For opt-out mechanisms available through ClairFi, please *see "Your Choices About How We Use and Disclose Your Information"* below.

How We Use Your Information

We use information that we collect about you or that you provide to us, including any personal information, to:

- Provide, operate, and improve the App and the ClairFi Services; match you with third-party Providers; administer onboarding, identity verification, KYC/AML checks, billing and subscription management; process payments and refunds through PCI-compliant payment processors; support Research Bot session processing and optional saving of outputs to the vault; maintain and secure your virtual vault and uploaded documents; detect, prevent and investigate fraud or abuse; comply with legal obligations and respond to legal requests; and, with your consent where required, send promotional communications.
- Fulfill and manage subscriptions, payments, billing, Provider engagements, and refunds in accordance with our Refund Policy. Subscription fees and any additional Provider fees are described at the point of sale. A PCI-DSS-compliant third-party payment processor processes payments on behalf of ClairFi. Refunds are available only where (a) no engagement letter has been executed with any Provider in the Virtual Family Office and (b) no investment or other billable activity has occurred through the platform; initial consultations with Providers do not disqualify a refund. Once an engagement letter has been executed or an investment has been made, the subscription is non-refundable. You can cancel your subscription at any time through the App; cancellation will stop future recurring charges, but it may not immediately delete your account data. For billing questions or refund requests, contact support at **privacy@clairfi.com**.
- Give you notices about your account and subscription, including expiration, renewal, and billing notices.
- Conduct our obligations and enforce our rights arising from any contracts entered into between you and us or between you and third-party Providers facilitated through the App, including for billing and collection.
- Notify you when App updates are available, and of changes to any products or services we offer or provide through it, including changes to the Research Bot, virtual vault, or third-party Provider offerings.
- Other legitimate business purposes consistent with this Privacy Policy and applicable law, such as internal analytics, fraud prevention, compliance, and customer support.

The usage information we collect helps us to improve our App and to deliver a better and more personalized experience by enabling us to:

- Estimate our audience size and usage patterns.
- Store information about your preferences, allowing us to customize our App according to your individual interests and to improve Provider matching.
- Speed up your searches and Research Bot queries.
- Recognize you when you use the App.

We use location information we collect to provide location-based Provider matching and localized services, to detect and prevent fraud and abuse, and to comply with legal or regulatory obligations where necessary.

We may use the contact information you provide to notify you about ClairFi's own products and services and, with your consent, to notify you about selected third-party Provider offerings. If you do not want us to use your contact information for marketing purposes, you may opt out at any time by adjusting your account preferences or by contacting us at **privacy@clairfi.com**. You may also use the unsubscribe link contained in marketing emails.

We do not currently display third-party advertising in the App. If we change this practice in the future, we will disclose such activity and provide required choices and opt-out mechanisms in accordance with applicable law.

Disclosure of Your Information

We may disclose aggregated or de-identified information about our users, as well as information that does not personally identify any individual or device, without restriction.

In addition, we may disclose personal information that we collect or you provide:

- To our subsidiaries and affiliates, if any, for the purposes described in this Privacy Policy and subject to appropriate confidentiality protections.
- To contractors, service providers, and other third parties we use to support our business *(e.g.,* hosting providers, payment processors, analytics vendors, identity-verification vendors, email delivery providers, and security vendors) who are bound by contractual obligations, including data processing addenda and confidentiality obligations, to keep personal information secure and to use it only for the purposes we specify.
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of ClairFi's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by ClairFi about our App users is among the assets transferred.
- To third parties to market their products or services to you only if you have affirmatively consented to such disclosures; where we permit such disclosures, we contractually require those third parties to keep personal information confidential and to use it only for the disclosed purposes.
- To fulfill the purpose for which you provide it.
- For any other purpose disclosed by us when you provide the information.

- With your consent.
- To Providers you select or are matched with through the App to enable those Providers to deliver professional services to you under separate engagement agreements (Providers are independent controllers or processors and are responsible for their own data practices; you should review each Provider's engagement agreement and privacy notice before sharing additional information).

We may also disclose your personal information:

- To comply with any court order, law, or legal process, including responding to any government or regulatory request.
- To enforce our rights arising from any contracts entered into between you and us (including under the App Terms of Use) and for billing and collection.
- If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of ClairFi, our customers, or others. This includes exchanging information with other companies and organizations to protect against fraud and reduce credit risk.

Choices About How We Use and Disclose Your Information

We strive to provide you with choices regarding the personal information you provide us. This section describes mechanisms we provide for you to control certain uses and disclosures of your information.

- **Tracking Technologies.** You can set your browser to refuse all or some browser cookies, or to alert you when cookies are being sent. You can opt out of certain tracking technologies and analytics by adjusting your account settings or by contacting **privacy@clairfi.com**. Please note that ClairFi does not currently utilize third-party tracking for behavioral advertising. If this changes, we will provide notice and opt-out mechanisms. We do not sell or share personal information for cross-context behavioral advertising, as defined under the CCPA/CPRA, nor do we sell covered information as defined under the Nevada Privacy Law. Any changes to this practice will be reflected in an updated policy and required California notices.
- **Location Information.** You can choose whether to allow the App to collect and use real-time information about your device's location through your device's privacy settings or via the App's account settings. If you block the use of location information, some parts of the App (including localized Provider matching) may become inaccessible or may not function properly.
- **Promotions by ClairFi.** If you do not want us to use your contact information to promote our own or third parties' products or services, you can opt out by adjusting your account settings, by using the unsubscribe link included in marketing emails, or by emailing **privacy@clairfi.com**.
- **Targeted Advertising by ClairFi.** We do not currently use the data we collect to deliver targeted advertising in a manner that would constitute a "sale" or "sharing" under applicable California law, and we do not engage in cross-context behavioral advertising. If we initiate targeted advertising in the future, we will provide notice and implement opt-out mechanisms as required by law.

- **Disclosure of Your Information for Third-party Advertising and Marketing.** We do not share personal data with unaffiliated third parties for interest-based advertising without your affirmative consent. If we change this practice, we will provide notice and opt-out options; until then, you may control promotional disclosures as described above.

We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide you with ways to choose not to have your information collected or used in this way. You can opt out of receiving targeted ads from members of the Network Advertising Initiative ("**NAI**") on the NAI's website.

Residents in certain states, including California and Nevada, have additional rights and choices regarding their personal information. These rights are detailed in the "Your State Privacy Rights" section below.

Accessing and Correcting Your Personal Information

You can review and change your personal information by logging into the App and visiting your account profile page. If you cannot access your account, you may submit a request to **privacy@clairfi.com** (subject line: "Access/Correction Request"). We will verify your identity before acting and will respond within the timeframes required by applicable law.

You may also send us an email at **privacy@clairfi.com** to request access to, correct, or delete any personal information that you have provided to us. We cannot delete your personal information except by also deleting your user account. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or result in incorrect information. We will verify your identity as reasonably necessary to fulfill your requests.

If you delete your User Contributions from the App, copies of your User Contributions may remain viewable in cached and archived pages or might have been copied or stored by other App users. The proper access and use of information provided on the App, including User Contributions, are governed by our Terms of Use, available at **https://www.clairfi.com/terms**.

For additional information about your privacy rights under California and Nevada law, please refer to the "Your State Privacy Rights" section below.

Your State Privacy Rights

State consumer privacy laws may provide their residents with additional rights regarding our use of their personal information.

In addition to the rights described below for California residents under the CCPA/CPRA, California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our App who are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an email to **privacy@clairfi.com** or write to us at: ClairFi Technologies Inc., 26077 Nelson Way, Ste 502, Katy, TX 77494, Attn: Privacy.

Many states, including California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia, provide (now or in the future) their state residents with rights to:

- Confirm whether we process their personal information.
- Access and delete certain personal information.
- Correct inaccuracies in their personal information, considering the information's nature and processing purpose (excluding Iowa and Utah).
- Data portability.
- Opt-out of personal data processing for:
    - targeted advertising (excluding Iowa);
    - sales; or
    - profiling in furtherance of decisions that produce legal or similarly significant effects (excluding Iowa and Utah).
- Either limit (opt-out of) or require consent to process sensitive personal data or process personal data of minors under 18, 17, or 16 years old.

The exact scope of these rights may vary by state. To exercise any of these rights, please submit a request through the ClairFi account portal (recommended) or by emailing **privacy@clairfi.com** with the subject line indicating the request type *(e.g.,* "Access Request," "Deletion Request," or "Opt-Out Request"). To appeal a decision regarding a consumer rights request, email **privacy@clairfi.com** with the subject line "Privacy Appeal." Our Privacy Team will review appeals and provide a written response. We will verify your identity as reasonably necessary and will respond within the timeframes required by applicable law.

Under Nevada Revised Statutes Chapter 603A, Nevada residents have the right to opt out of the sale of certain personal information to third parties who will sell or license their information to others. This right applies even if we do not currently sell personal information. Residents who wish to exercise this right may submit a request to **privacy@clairfi.com** or through the ClairFi account portal. However, please note that we do not currently sell personal data that triggers Nevada's opt-out requirements under NRS 603A.

Data Security

We implement commercially reasonable administrative, technical, and organizational measures designed to protect personal information from accidental loss and from unauthorized access, use, alteration, or disclosure. These measures include, as applicable: TLS 1.2 or higher for data in transit; encryption at rest for sensitive data *(e.g.,* AES-256 where used); documented encryption key management and rotation practices; role-based access controls and least-privilege permissions; multi-factor authentication for privileged accounts; secure logging and monitoring;

regular vulnerability scanning, penetration testing, and patch management; periodic third-party security assessments and audits (including SOC 2 Type II where maintained); and contractual, technical, and organizational safeguards with sub processors. Payment transactions are encrypted in transit and processed by PCI-DSS compliant third-party payment processors; ClairFi does not retain full payment card numbers outside of those processors. Personal data stored in the ClairFi virtual vault (including any IRS-designated vault) is subject to enhanced encryption, separate keying and access controls, strict role-based approvals, and limited access that is available only to you and those you authorize, or as required by law; IRS-related tax records in the vault are retained in accordance with our IRS retention framework and applicable tax-record retention laws. The Research Bot processes inputs in isolated sessions; session inputs are deleted at the end of each session unless you expressly elect to save outputs to your secure vault or unless retention is necessary for troubleshooting, fraud investigation, legal process, or to satisfy a statutory obligation. We do not send Research Bot inputs to public internet search engines and do not use Research Bot session inputs to train ClairFi production models absent explicit disclosure and affirmative consent. ClairFi does not sell or share personal information for cross-context behavioral advertising and does not share personal information in a manner that constitutes a "sale" or "sharing" under the CCPA/CPRA. We will maintain and publish our choices and opt-outs in a manner consistent with applicable law.

The safety and security of your information also depend on you. When we have given you (or you have chosen) a password or other credential to access parts of our App, you are responsible for keeping that credential confidential and for all activity that occurs under your account. You must not share your credentials with anyone. Where multi-factor authentication (MFA) is available, you should enable and maintain MFA to help protect your account; ClairFi may require MFA for privileged, high-risk, or accreditation-verified accounts. Do not post account credentials or other sensitive information in public areas of the App; information you share in public or shared areas may be visible to other users. You should also avoid uploading unnecessary highly sensitive personal information *(e.g.,* full Social Security numbers, full bank account passwords, or other authentication credentials) into non-vault areas of the platform or into Research Bot sessions; if you choose to provide such information, you do so at your own risk and consent to the processing described in this policy. ClairFi's Services are intended for persons who are 18 years of age or older, who reside in the United States or its territories, and for certain Services (including investment offerings) for users who qualify as accredited investors as defined by applicable securities laws and regulations, where required; do not create an account if you do not meet any applicable eligibility requirements. ClairFi may suspend or restrict access to accounts if we reasonably suspect account compromise, unauthorized sharing of credentials, misrepresentation of accreditation or eligibility, or other misuse.

Unfortunately, no transmission of information over the internet or mobile networks is entirely secure. Although we employ industry-standard safeguards to protect your personal information, we cannot guarantee the absolute security of information transmitted to or from the App. Any transmission of personal information is at your own risk. We are not responsible for the circumvention of any privacy settings or security measures by third parties. In the event of a security incident involving personal data, we will follow our incident response procedures and provide notice to affected users and regulators as required by applicable law; such notice will include timely individual notice where required and statutory notifications to regulators *(e.g.,* some statutes require notice without unreasonable delay and certain state laws specify a deadline

such as within 30–60 days of discovery). We will also coordinate breach responses with law enforcement and other relevant authorities as necessary. We will comply with any specific notification obligations (including, where applicable, IRS and tax authorities for incidents affecting tax records).

Changes to Our Privacy Policy

We reserve the right to update this Privacy Policy from time to time. If we make material changes to how we treat users' personal information, we will provide notice by email to the primary email address associated with your account (unless you have opted out of such communications) and by posting a prominent notice within the App (or on the applicable Services page) together with an updated "Last updated" date; where required by law for particular users or jurisdictions, we will provide additional notice *(e.g.,* by postal mail or other statutorily required methods). Material changes that affect your legal rights or material changes in how we use your personal information will be highlighted and, where required by law, will be made effective only after the legally required notice period *(e.g.,* a 30-day notice for certain changes where contract or notice rules apply) or upon your affirmative consent if consent is legally required. We will make this policy available in alternate accessible formats upon request *(e.g.,* large print, accessible HTML, or other formats). We will provide instructions for requesting an accessible version in the Contact Information section below. For non-material changes, we will update the policy on the Services and indicate the revised "Last updated" date.

We indicate the date of our last update to this privacy policy at the top of the page. You are responsible for ensuring that we have an up-to-date, active, and deliverable email address and phone number for you, and for periodically reviewing this privacy policy to check for any changes. If you require an accessible format of this policy, please contact us using the methods in the Contact Information section and indicate the requested format.

Contact Information

To exercise your rights, to ask questions about this privacy policy, or to contact us about our privacy practices, please contact ClairFi Technologies Inc. via e-mail at privacy@clairfi.com or via regular postal mail at the following mailing address:

ClairFi Technologies Inc.
Attn: Privacy Team
26077 Nelson Way, Suite 502
Katy, TX 77494

For privacy requests and inquiries, please contact us by email at **privacy@clairfi.com**. Additional contact methods may be available based on your jurisdiction and the nature of your request.

To register a complaint or concern, please submit a detailed description of your issue to **privacy@clairfi.com**. We will acknowledge receipt and attempt to resolve the complaint. If you are a California resident and your complaint remains unresolved after 45 days, you may contact the California Attorney General's office. Nothing in this policy limits your right to file a

complaint with relevant regulatory authorities. For other jurisdictions, we will provide contact information for the appropriate supervisory authority upon request.

California Privacy Notice (CCPA/CPRA)

This California-specific notice explains how ClairFi Technologies Inc., doing business as ClairFi (collectively, "**ClairFi**," "**Company**," "**we**," "**our**," or "**us**"), collects, uses, discloses, retains, sells, shares, and otherwise processes personal information of California residents as required by the California Consumer Privacy Act as amended by the California Privacy Rights Act (collectively, "**CCPA/CPRA**"). ClairFi operates a technology platform and marketplace (the "**Services**") that connects users with independent third-party financial, tax, legal, and related professional service Providers (the "**Providers**"). ClairFi provides platform infrastructure, matching, a secure virtual vault, an AI-powered Research Bot, subscription and billing services, and related administrative features; Providers are independent contractors or entities and remain responsible for the personal information they collect, process, and retain in performing professional services under separate engagement agreements. This notice supplements our general Privacy Policy and applies to California residents. Any terms defined in the CCPA/CPRA have the same meaning when used in this notice.

The California-specific portions of this Privacy Policy do not apply to ClairFi's collection and use of personal information in the context of employment, as an applicant, contractor, or other workforce member. Employees, job applicants, contractors, interns, and other workers should consult ClairFi's Employee/Workforce Privacy Notice, located on the Company's intranet.

This Notice applies only to California residents. Consumers residing outside California should refer to ClairFi's general Privacy Policy available on our website.

Personal Information Collected

We collect and use information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household ("**personal information**"). Personal information does **not** include:

- Publicly available information, including from government records, through widely distributed media, or that the consumer made publicly available without restricting it to a specific audience.
- Lawfully obtained, truthful information that is a matter of public concern.
- Deidentified or aggregated consumer information.
- Certain categories of information excluded from the CCPA/CPRA scope, such as: information subject to the Health Insurance Portability and Accountability Act (HIPAA) and the California Confidentiality of Medical Information Act (CMIA), clinical trial data, and sector-specific regulated data (e.g., information governed exclusively by the Fair Credit Reporting Act (FCRA) or the Gramm-Leach-Bliley Act (GLBA)), where the law provides such an exclusion.

- health or medical information covered by the Health Insurance Portability and Accountability Act (HIPAA) and the California Confidentiality of Medical Information Act (CMIA), clinical trial data, or other qualifying research data; or
- personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act.

Personal Information Categories Chart

The chart below identifies the categories of personal information we have collected from California residents in the twelve (12) months preceding the Effective Date, along with the typical retention periods used by ClairFi for such categories (subject to legal, regulatory, or contractual exceptions described elsewhere in this notice and in our Privacy Policy).

Category	Examples	Collected	Typical Retention Period
Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes.	Retained for the duration of your active account and for up to 5 years after account termination for business, compliance, and dispute-resolution purposes, except where a longer statutory retention period applies (e.g., tax or regulatory records).
Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) ("**California Customer Records**").	A name, signature, Social Security number, physical characteristics or description, photograph, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Yes.	Retention varies by subcategory: identity and onboarding documents are retained for the active account period and up to 5 years after account termination for business and compliance purposes; tax and IRS-related documents stored in the ClairFi IRS vault are retained for up to 7 years to satisfy IRS and tax-record retention obligations unless a different statutory period applies.

Category	Examples	Collected	Typical Retention Period
Protected classification characteristics under California or federal law ("**Protected Classes**").	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, reproductive health decision making, military and veteran status, or genetic information (including familial genetic information).	Yes, to the extent you provide such information, or necessary for a Service (*e.g.*, voluntary demographic information used for matching and personalization).	Retained for the duration of the account and up to 5 years after account termination, unless a different legal or contractual retention requirement applies.
Commercial information.	Records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Yes.	Retained for the duration necessary to support billing, refunds, regulatory and tax compliance, and fraud prevention; up to 5 years after account termination for compliance and audit purposes, subject to legal requirements.
Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	No. ClairFi does not routinely process biometric information for platform purposes, except where you expressly consent for a narrowly scoped verification feature.	If we collect biometric information with explicit consent for verification purposes, we will retain it only for that purpose and in accordance with any applicable legal requirements. Any such collection will be disclosed with a separate notice and will require explicit consent where required by law.

Category	Examples	Collected	Typical Retention Period
Internet or other similar network activity.	Activity on our websites, mobile apps, or other digital systems, such as internet browsing history, search history, system usage, electronic communications with us, postings on our social media sites.	Yes. We collect device, technical, and usage information to operate and secure the Services, as well as for analytics and service improvement purposes. We presently do not use cookies or other trackers.	Retained for operational and security purposes for the duration necessary to provide the Services and for up to 5 years after account termination for logs and security investigations, subject to specific vendor retention terms.
Geolocation data.	Physical location or movements, such as the time and physical location related to use of our internet website, application, or device.	No, we do not collect precise geolocation routinely. We may collect general location information (*e.g.*, city or state) or precise geolocation data only if you explicitly enable a feature for a specific Service, and we will disclose that at the point of collection.	If we collect precise geolocation with your consent for a specific feature, we will retain it only to provide that feature and in accordance with our general retention rules and any applicable law.
Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	Yes, if you provide images, voice recordings, or videos for identification, onboarding, Provider interactions, or customer service; and	Retained only for the purpose that we collected (e.g., onboarding, verification, or support) and in accordance with our retention schedules; we tie typical retention to account lifecycle and up to 5 years after account termination for investigation and compliance purposes.

Category	Examples	Collected	Typical Retention Period
		if we provide notice and consent to record or monitor calls.	
Professional or employment-related information.	Current or past job history.	Yes, where you provide professional or employment information for matching, profiling, or to receive Services from Providers.	Retained for the duration necessary to provide the Services and for up to 5 years after account termination, unless otherwise required by law or contract.
Inferences drawn from other personal information.	A profile reflects a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Yes. We may generate inferences to facilitate Provider matching, personalization, service improvement, and analytics.	Retained for service improvement and matching; aggregated or de-identified inferences may be retained indefinitely for analytics. Personal-identifiable inferences are retained no longer than necessary for the purposes described herein.
Sensitive personal information.	Further identified in the sensitive categories chart below. Under the CCPA/CPRA, certain categories of information are treated as "sensitive" and may receive heightened protections; ClairFi limits collection and use of sensitive categories to what is necessary for onboarding, billing, tax, Know Your Customer (KYC)/Anti-Money Laundering (AML), and required Provider services.	Yes. Certain sensitive personal information categories (such as government identifiers, tax identifiers, and financial account details) are collected and processed only where necessary and subject to enhanced protections and, where required,	Retention depends on the specific sensitive category and legal obligations (e.g., IRS vault records: up to 7 years; other sensitive data: retained for the active account period and up to 5 years thereafter, unless law requires otherwise).

Category	Examples	Collected	Typical Retention Period
		opt-in/consent mechanisms.	

Sensitive Personal Information Categories Chart

We obtain the categories of personal information listed above from the following categories of sources, as applicable to a particular customer and Service:

The chart below identifies the sensitive personal information categories, if any, that we have collected from consumers to infer characteristics about them in the last 12 months and the typical retention for each category.

Sensitive Personal Information Category	Collected to Infer Characteristics?	Typical Retention Period
Government identifiers, such as your Social Security number (SSN), driver's license, state identification card, or passport number.	Yes. Collected where required for identity verification, KYC/AML, tax filing, or IRS compliance.	Retained for the duration of your active account and for up to 5 years after account termination for business, compliance, and dispute-resolution purposes, except where a longer statutory retention period applies (e.g., tax or regulatory records).
Complete account access credentials, such as usernames, account logins, account numbers, or card numbers, combined with the required access/security code or password.	Yes. We process account credentials and payment/account numbers to authenticate accounts and to process payments (PCI DSS-compliant third-party payment processors process payments themselves).	Retention varies by subcategory: identity and onboarding documents are retained for the active account period and up to 5 years after account termination for business and compliance purposes; tax and IRS-related documents stored in the ClairFi IRS vault are retained for up to 7 years to satisfy IRS and tax-record retention obligations unless a different statutory period applies.
Precise geolocation, such as physical store visits or physical locations when visiting websites or using mobile apps.	No, we do not collect precise geolocation routinely. We may collect general location information (*e.g.*, city or state) or precise geolocation data only if you explicitly	If we collect precise geolocation with your consent for a specific feature, we will retain it only to provide that feature and in accordance with our general retention rules and any applicable law.

Sensitive Personal Information Category	Collected to Infer Characteristics?	Typical Retention Period
	enable a feature for a specific Service, and we will disclose that at the point of collection.	
Racial or ethnic origin.	Yes, to the extent you provide such information, or necessary for a Service (*e.g.*, voluntary demographic information used for matching and personalization).	Retained for the duration of the account and up to 5 years after account termination, unless a different legal or contractual retention requirement applies.
Citizenship or immigration status.	Yes, to the extent you provide such information, or necessary for a Service (*e.g.*, voluntary demographic information used for matching and personalization).	Retained for the duration of the account and up to 5 years after account termination, unless a different legal or contractual retention requirement applies.

Sources of Personal Information

Directly from you when you create an account, complete forms, upload documentation to the virtual vault, provide information to the Research Bot or to Providers, or otherwise interact with the Services.

- Indirectly from you through your interactions with the Services, including account activity, device and usage data, and correspondence with our support or Provider teams, and from Providers when acting on your instructions.
- From our service providers and sub-processors (*e.g.*, hosting, analytics, identity verification, payment processors, and customer support providers) that assist us in delivering the Services.
- From Providers, where a Provider collects or shares information with ClairFi for the purpose of facilitating or delivering Services you requested.
- From publicly available sources and, where applicable, data you elect to import or link to the Services (*e.g.*, third-party accounts or professional directories) and from other third parties with your consent.
- From other sources where you, your agent, or an authorized third party provides data to ClairFi while receiving Services (*e.g.*, referrals or introductions facilitated through the platform).
- From in-Service or third-party tools you use in conjunction with the Services, subject to the terms you authorize and the Provider's own privacy practices.
- Where a Provider or other third party provides a separate privacy notice in connection with a Service, that notice governs that party's processing of personal information in relation to that Service; please review Provider notices and engagement agreements before sharing information with a Provider.
- Other sources where we have lawful grounds to process your personal information in connection with the Services.

How We Use Personal Information

Personal Information Collection, Use, and Disclosure Purposes

We may use and disclose the personal information, including sensitive personal information, we collect to advance our business and commercial purposes, specifically to:

- Develop, offer, and provide you with our services, including operating our subscription services, matching you with independent third-party Providers in the ClairFi Virtual Family Office, and providing platform features such as the secure virtual vault and the AI-powered Research Bot.
- Meet our obligations and enforce our rights arising from any contracts with you, including for billing, collections, payment processing, tax reporting, and other regulatory or compliance requirements.
- Fulfill the purposes that you provided your personal information or that were described to you at collection, and as the CCPA otherwise permits.
- Improve our platform and Services and enhance marketing, customer relationships, and user experience.

- Notify you about changes to our Services or policies.
- Administer our systems and conduct internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes, identity verification, KYC/AML, and fraud prevention, and other compliance activities necessary to operate the Services.
- Enable your participation in our website's and mobile apps' interactive features and other platform functionality.
- Protect our Company, employees, users, and operations, including preventing, detecting, and responding to security incidents, abuse, or other malicious activity.
- Send promotional communications or other information about our Services where you have consented or as otherwise permitted by law. ClairFi does not use, disclose, sell, or share personal information for cross-context behavioral advertising or targeted advertising purposes. We do not engage in automated decision-making that produces legal or similarly significant effects concerning consumers.
- Provide service-related suggestions and recommendations to you (*e.g.*, recommended Providers or Service features) where such suggestions are consistent with your account, your indicated preferences, and applicable consent and privacy settings.
- Manage your consumer relationship with us, including online account creation, maintenance, and security, or for matters concerning your account or Service interactions; and
- Perform data analytics, benchmarking, and service-improvement analysis in aggregate or de-identified form where possible.
- Administer and maintain our systems and operations, including detecting and mitigating security risks.
- Engage in corporate transactions requiring review of consumer records, such as for evaluating potential Company mergers, acquisitions, or sales of assets.
- Comply with applicable laws and regulations and respond to lawful requests from regulators or law enforcement.
- Exercise or defend our legal rights and those of our employees, affiliates, customers, contractors, and agents.
- Respond to law enforcement requests and as required by applicable law or court order.

Sensitive Personal Information Use and Disclosure Purposes

We may use or disclose sensitive personal information for the following statutorily approved reasons **(Permitted SPI Purposes)**:

- Performing actions that are necessary for our consumer relationship and that an average consumer in a relationship with us would reasonably expect.
- Preventing, detecting, and investigating security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information.
- Defending against and prosecuting those responsible for malicious, deceptive, fraudulent, or illegal actions directed at us.
- Ensuring physical safety, including the safety of data centers, facilities, and personnel where necessary.

- Short-term, transient use, such as non-personalized advertising shown as part of your current interactions with us, provided we do not disclose the sensitive personal information to another third party and do not use it to build a profile about you or otherwise alter your experience outside your current interaction with us.
- Services performed for us, including maintaining or servicing accounts, processing or fulfilling transactions, verifying consumer information, processing payments, or providing financing, analytic services, storage, or similar services for us.
- Activities required to verify or maintain the quality of a service that we own provide, or to improve, upgrade, or enhance such service.
- In particular, on a platform that connects users with financial, tax, legal, and related Providers, ClairFi may collect and process sensitive personal information that includes: taxpayer identifiers and tax documentation (including Social Security numbers or taxpayer identification numbers where required for IRS or tax compliance), bank and payment account details (partial or full where necessary for payment processing), investment account and portfolio information, income and financial profile data, and other financial or transaction records. We process this information only as necessary to: (a) operate subscriptions and process payments; (b) match and facilitate the delivery of Provider services; (c) satisfy IRS, tax-reporting, and other regulatory obligations; (d) perform identity verification, KYC/AML, and fraud prevention; and (e) comply with the Permitted SPI Purposes described above. Research Bot inputs that contain sensitive personal information are treated as described elsewhere in this policy (session deletion unless you elect to persist outputs in the vault) and are protected with encryption and access controls.

We do not use or disclose sensitive personal information for purposes other than the Permitted SPI Purposes, except as described in this policy. To the extent the CPRA grants you the right to limit our use or disclosure of your sensitive personal information for certain purposes, you may exercise that right as described in the Your Rights and Choices section below.

Additional Categories or Other Purposes

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice. If required by law, we will also seek your consent before using your personal information for a new or unrelated purpose.

We may collect, process, and disclose aggregated or de-identified consumer information for any purpose, without restriction. When we collect, process, or disclose aggregated or de-identified consumer information, we will maintain and use it in de-identified form and will not attempt to re-identify the information, except to determine whether our de-identification processes satisfy any applicable legal requirements.

Disclosing, Selling, or Sharing Personal Information

Business Purpose Disclosures

We may disclose the personal information we collect, including sensitive personal information, to third parties for the business purposes described in the Personal Information Collection, Use, and Disclosure Purposes section. Typical recipients include independent third-party Providers you select or are matched with (who are generally independent controllers with respect to the personal information they collect directly from you), service providers and sub processors (such as hosting providers, payment processors, identity-verification vendors, analytics vendors, security vendors, and email delivery services), legal and regulatory authorities when required, affiliates in the context of corporate transactions, and professional advisors retained by ClairFi. We make business-purpose disclosures only underwritten contracts that describe the purposes, require recipients to keep the personal information confidential, prohibit using the disclosed information for any purpose except to perform the contract, and meet applicable CCPA/CPRA service-provider requirements.

Below, we identify the principal categories of third-party recipients and the general categories of personal information we disclose to them for business purposes in connection with operating the Services and administering accounts. For specific disclosures related to a given Provider or transaction, you should review the Provider's privacy notice and the applicable engagement agreement.

Business Purpose Disclosure: Principal Recipient Categories and Purposes

Principal recipient categories include: (1) Independent third-party. Providers in the ClairFi Virtual Family Office (personal information disclosed to Providers is used to perform the Provider's professional services under separate engagement agreements); (2) payment processors and financial institutions (to process subscription and Provider payments and for tax/reporting compliance); (3) hosting, cloud, and security vendors (to store, encrypt, and secure data); (4) identity verification, KYC/AML, and fraud-prevention; (5) analytics and service-improvement vendors (generally on an aggregated or deidentified basis where possible); (6) professional advisors, auditors, and insurers; and (7) regulators, courts, or law enforcement as required by law. The personal information categories disclosed to these recipients are the categories described in this policy (*e.g.*, identifiers, payment and billing information, account and subscription information, financial and tax records, and other content you provide). These disclosures are made for the business purposes described above (*e.g.*, to provide Services, process payments, verify identities, secure and maintain systems, and comply with legal obligations).

	Personal Information Categories Disclosed	**Sensitive Personal Information Categories Disclosed**	**Business Purpose Disclosures**

Customer Service Support Providers	A. Identifiers. B. California Customer Records. C. Commercial Information. D. Biometric information. E. Internet or other similar network activity. F. Geolocation data. G. Inferences.	K.1. Government identifiers. K.2. Complete account access credentials. K.3. Precise geolocation. K.8. Mail, email, or text message contents not directed to us.	To support customers with using our services, including online account management and troubleshooting.

Selling or Sharing Personal Information

We do not sell your personal information, including sensitive personal information, to third parties and have not sold it in the preceding 12 months. We do not share personal information with third parties for cross-context behavioral advertising purposes and have not shared personal information for that purpose in the preceding 12 months.

We do not sell or share the personal information of consumers we know to be under age 16. Where applicable, ClairFi will comply with CPRA/CCPA special rules regarding minors and obtain affirmative opt-in consent where required by law.

Your Rights and Choices

The following rights are available to California residents under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). Residents of other states may have similar rights under their applicable state laws:

Right to Know and Data Portability Requests

You have the right to request that we disclose certain information to you about our collection and use of your personal information (the "**right to know**"), including the specific pieces of personal information we have collected about you (a "**data portability request**"). Our response will cover the 12 months preceding the date of the request. You may exercise your right to know, including data portability requests, up to two times within 12 months. Once we receive your request and confirm your identity (see How to Exercise Your Rights), we will disclose to you:

- The categories of personal information we collected about you, and the sources from which we collected your personal information.

- The business or commercial purpose for collecting your personal information and, if applicable, whether we sold or shared that personal information.
- If applicable, the categories of persons, including third parties, to whom we disclose your personal information, including separate disclosures identifying the categories of your personal information that we disclosed for a business purpose to each category of persons; and sold or shared to each category of third parties, where applicable.
- When your right to know submission includes a data portability request, a copy of your personal information in a readily usable format, subject to any permitted redactions.

For more on exercising this right, see Exercising the Rights to Know, Delete, or Correct.

Right to Delete and Right to Correct

You have the right to request that we delete personal information that we collected from you and retain, subject to certain exceptions and limitations (the "**right to delete**"). Once we receive your request and confirm your identity, we will delete your personal information from our systems unless an exception allows us to retain it. To the extent required or practicable, we will notify our service providers and, where feasible, Providers in the Virtual Family Office to take appropriate action to delete your information from their systems.

You also have the right to request correction of personal information we maintain about you that you believe is inaccurate (the "**right to correct**"). We may require you to provide documentation, if needed, to confirm your identity and support your claim that the information is inaccurate. Unless an exception applies, we will correct personal information that our review determines to be incorrect and notify our service providers and, where feasible, the Providers to take appropriate action.

For more on exercising these rights, see Exercising the Rights to Know, Delete, or Correct.

Right to Limit Sensitive Personal Information Use and Disclosure to Permitted SPI Purposes

You have the right to request that businesses that use or disclose your sensitive personal information limit those actions to the CCPA/CPRA's Permitted SPI Purposes (the "**right to limit**"). Upon receipt of a valid request, ClairFi will limit the use and disclosure of your sensitive personal information to the CCPA/CPRA's Permitted SPI Purposes (e.g., identity verification, tax and regulatory compliance, onboarding, and fraud prevention). For more on the Permitted SPI Purposes and how we use sensitive personal information, see Sensitive Personal Information Use and Disclosure Purposes.

For more on the Permitted SPI Purposes and our additional use purposes, see Sensitive Personal Information Use and Disclosure Purposes.

Personal Information Sales or Sharing Opt-Out and Opt-In Rights

You have the right to opt out of the sale or sharing of your personal information. ClairFi does not sell or share personal information for cross-context behavioral advertising or otherwise in a manner that constitutes a "sale" or "sharing" under the CCPA/CPRA. If ClairFi's practices

change in the future, we will provide advance notice and a mechanism to exercise opt-out rights in accordance with applicable law.

Because we do not sell or share consumers' personal information as defined under the CCPA/CPRA or Nevada Revised Statutes Chapter 603A, the right to opt out of sale or sharing does not presently apply to our business practices. If that changes, we will update this policy and provide the required opt-out and opt-in mechanisms and notices in accordance with applicable state laws.

Right to Non-Discrimination

You have the right not to be discriminated against or retaliated against for exercising any of your privacy rights under applicable privacy laws, including but not limited to the CCPA/CPRA and similar state privacy regulations.

How to Exercise Your Rights

Exercising the Rights to Know, Delete, or Correct

To exercise your privacy rights under applicable state laws, including but not limited to rights to know, data portability, deletion, or correction under the CCPA/CPRA, or opt-out rights under Nevada law, please submit a verifiable request to us by one of the following methods:

- Emailing us at **privacy@clairfi.com**.
- Mailing a verifiable request to: ClairFi Technologies Inc., 26077 Nelson Way, Ste 502, Katy, TX 77494, Attn: Privacy.
- You may also designate an authorized agent to submit a request on your behalf; see Verification Process and Authorized Agents below for details.

Please describe your request with sufficient detail so we can properly understand, evaluate, and respond to it. You or your authorized agent may submit a request to know, including data portability, up to two times within any 12 months.

Exercising the Right to Limit or Opt-Out

If you are a California resident, you can submit your request to limit the use of your sensitive personal information or to opt-outopt-out of a sale/sharing (to the extent applicable) through any of the following methods:

- Emailing **privacy@clairfi.com** .
-
- Mailing a request to ClairFi Technologies Inc., 26077 Nelson Way, Ste 502, Katy, TX 77494, Attn: Privacy.

You can also submit your request to opt out of personal information sales or sharing through an opt-out preference signal (e.g., the Global Privacy Control), where we can reasonably authenticate and verify the signal.

Notice of Right to Opt-out of Sale/Sharing:

Verification Process and Authorized Agents

Only you, or someone legally authorized to act on your behalf, may make a request to know, delete, or correct information related to your personal information. To designate an authorized agent, you must provide a signed authorization that identifies the agent and the scope of the authorization, and the agent must supply proof of their identity. If you are requesting on behalf of a minor, we will require proof of parental or guardian authority. To verify identity, we may request information reasonably necessary to process the request (e.g., name, email address, account username, and a copy of a government-issued photo ID or other documentation), and we will only use that information to verify the requester's identity or authority to act. We may treat requests submitted from a password-protected account as sufficiently verified when the request relates to the personal information associated with that account.

We cannot respond to your request to know, delete, or correct if we cannot verify your identity or authority to make the request, and confirm the personal information relates to you. We will only use personal information provided in the request to verify the requester's identity or authority to make the request.

We consider requests made through your ClairFi password-protected account sufficiently verified when the request relates to the personal information associated with that specific account. You do not need to create an account with us to submit a request to know, correct, or delete, except where account authentication is necessary to verify the request.

For requests to limit use/disclosure, or to opt out, we will ask for the information necessary to complete the request, which may include, for example, the consumer's name, email address, account username, or other identifying details necessary to locate the relevant records.

Responding to Your Requests to Know, Delete, or Correct

We will confirm receipt of your request within ten business days. If you do not receive confirmation within that timeframe, please contact **privacy@clairfi.com**.

We will endeavor to substantively respond to a verifiable request within 45 calendar days (90 calendar days total) of its receipt. If we require additional time (up to 45 calendar days), we will notify you in writing of the reason for the extension and the extension period. We will deliver our written response to your verified email address, via your password-protected account, or by mail to the address you provide when necessary. Our substantive response will explain whether and how we have complied with your request, and if we cannot comply in whole or in part, we will provide the reason, subject to any applicable legal or regulatory restrictions.

Any disclosures we provide will cover information for the 12 months preceding the date the request is received. We will consider requests for a longer disclosure period where feasible and where not inconsistent with applicable law.

For data portability requests, we will provide your personal information in a readily usable, machine-readable format (e.g., CSV or JSON) that should allow you to transmit the information from one entity to another without hindrance.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that a fee is warranted, we will explain the reason and provide a cost estimate before processing your request.

Response and Timing on Rights to Limit or Opt-Out

For California residents, in response to your request to limit the use of your sensitive personal information or to opt out of the sale or sharing of your personal information under the CCPA/CPRA, we will process your request within 15 business days from receipt. For Nevada residents exercising opt-out rights under NRS 603A, we will process your request within 60 days from receipt. You do not need to create an account with us to exercise these rights. We will only use the personal information provided with your request to verify your identity and to comply with the request.

We will notify our service providers, contractors, and other relevant downstream recipients that process personal information on our behalf of your request where necessary for them to comply, and we will instruct them to (a) comply with your request and (b) forward the request to their downstream recipients only when required to effectuate compliance. Our service providers are contractually required to assist us and comply with such requests to the extent applicable under their agreements with us and applicable law.

We may deny limitation or opt-out requests if we have a good-faith, reasonable, and documented belief that the request is fraudulent or not from the consumer to whom the information relates. If we deny a request, we will notify you of the denial and provide, to the extent required by law, the reason for the denial and instructions for how to appeal or resubmit the request with additional verification.

You can confirm that we processed your request by checking your ClairFi account settings at https://**www.clairfi.com/account** or by contacting us at **privacy@clairfi.com**. Where applicable, your account settings will display controls indicating that we have limited the use of your sensitive personal information and that we do not sell or share your personal information.

Once you request to limit the use of your sensitive personal information or to opt out of sale/sharing, we will not seek reauthorization for at least 12 months to use or disclose your sensitive personal information for purposes other than the Permitted SPI Purposes. You may opt back in at any time by following the opt-in instructions below.

To opt back in, you may update your preferences in your ClairFi account at **https://www.clairfi.com/account** or contact us at **privacy@clairfi.com** with a written request to opt back in.

Reselling or Resharing Personal Information

ClairFi does not sell or share personal information for cross-context behavioral advertising and does not engage in reselling or resharing of personal information in a way that would trigger obligations under either the California CCPA/CPRA or Nevada NRS 603A. If our practices change and we begin to sell or share personal information as defined under applicable law, we

will provide explicit advance notice, publish opt-out instructions, and provide any required third-party opt-out links or mechanisms in our California-specific notice.

How We Protect Your Personal Data

We use commercially reasonable administrative, technical, and physical safeguards designed to protect your personal data from accidental loss, misuse, unauthorized access, disclosure, alteration, and destruction. These safeguards include encryption in transit (TLS 1.2 or higher) and encryption at rest (e.g., AES-256 where used), role-based access controls and least-privilege access, multi-factor authentication for privileged accounts, secure logging and monitoring, regular vulnerability scanning and patching, periodic third-party penetration testing and audits, employee security training, and contractual security obligations with our sub-processors. We maintain SOC 2 Type II certification and require our service providers to maintain appropriate security measures. However, no website, mobile application, system, electronic storage, or online service is completely secure, and we cannot guarantee the absolute security of personal data transmitted to or stored by us; any transmission of personal data is at your own risk.

The safety and security of your information also depend on you. You are responsible for maintaining the confidentiality of your account credentials, selecting a strong password, enabling multi-factor authentication where available, avoiding sharing your credentials with others, promptly notifying us of any unauthorized use of your account, and exercising care in what personal data you choose to share through non-vault channels (e.g., in Research Bot sessions or unencrypted communications).

CCPA Rights Request Metrics

We publish metrics regarding CCPA/CPRA consumer rights requests as required by law. These metrics are available upon request by contacting privacy@clairfi.com. To request metrics regarding CCPA/CPRA consumer rights requests we received for a specific calendar year, please contact **privacy@clairfi.com** and specify the requested year(s). ClairFi may publish these metrics in the future in our California-specific notice.

Privacy Policy Changes

We reserve the right to update this Privacy Policy at any time. When we make material changes to this Privacy Policy, we will update the "Last updated" date shown at the top of the policy and, where required by law or for material changes that affect your rights, provide additional notice, such as an in-service notice or an email to the address associated with your account. We encourage you to review this Privacy Policy periodically to stay informed of any changes.

Contact Information

If you have any questions or comments about this policy, the ways that we collect and use your information, or your choices and rights regarding such use, or if you wish to exercise your rights under California law, please contact us as follows:

Website: **https://www.clairfi.com/privacy**
Email: **privacy@clairfi.com**

Postal Address:

ClairFi Technologies Inc.
Attn: Privacy
26077 Nelson Way, Ste 502, Katy, TX 77494

If you need to access this Privacy Policy in an alternative format due to a disability, please contact us at **privacy@clairfi.com**. We will make reasonable efforts to provide the policy in an alternative, accessible format upon request.