FAST CREDIT UNION

California Privacy Policy (CCPA/CPRA)

Effective Date: May 1, 2026
Last Updated: May 1, 2026

YOUR PERSONAL INFORMATION PROTECTIONS

What Does FAST Credit Union Do With Your Personal Information?

FAST Credit Union ("FAST," "we," "our," or "us") respects the privacy of our members and website users. We recognize the importance of maintaining the confidentiality and security of your personal and financial information.

This Privacy Policy explains how we collect, use, share, and protect your personal information in accordance with:

- The **California Consumer Privacy Act (CCPA)**
- The **California Privacy Rights Act (CPRA)**
- The **Gramm-Leach-Bliley Act (GLBA)**

WHAT IS PERSONAL INFORMATION?

Under California law, "Personal Information" means information that identifies, relates to, or could reasonably be linked to you or your household. This includes:

- Identifiers (name, address, email, IP address)
- Protected Classifications (age, gender)
- Government identifiers (SSN, driver's license)
- Financial information (account numbers, transaction history)
- Internet activity (browsing behavior, website interactions)
- Geolocation data
- Biometric information (e.g., voiceprints used for identity verification)
- Employment or education data

WHAT IS SENSITIVE PERSONAL INFORMATION?

Sensitive Personal Information includes:

- Social Security number
- Account credentials (username/password, PIN)
- Financial account access data
- Precise geolocation
- Biometric identifiers (including voice recognition data)
- Contents of communications (where applicable)

CATEGORIES OF PERSONAL INFORMATION WE COLLECT

We may collect the following categories:

1. Personal Identifiers

- Name, email, phone number
- Address and date of birth
- IP address and device identifiers

2. Account & Financial Information

- Account numbers and balances
- Transaction history
- Credit history and creditworthiness

3. Internet & Usage Data

- Website usage and interactions
- Cookies and session data

4. Biometric Information (Voice Verification)

- Voice recordings and voiceprints used to authenticate your identity
- Metadata associated with voice authentication sessions

5. Sensitive Personal Information

- Social Security number
- Login credentials
- Biometric identifiers

CATEGORIES OF PERSONAL INFORMATION WE COLLECTED WITHIN THE LAST TWELVE (12) MONTHS

Category	Examples	Collected
A. Identifiers.	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.
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	Name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.	Yes.
C. Protected classification characteristics under California or federal law.	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, veteran or military status, genetic information (including	Yes.

	familial genetic information).	
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Yes.
E. 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.	Yes.
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	Yes
G. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	No

HOW WE COLLECT YOUR INFORMATION

We collect information:

- Directly from you (applications, forms, phone calls)
- Automatically (website usage, cookies)
- From third parties (credit bureaus, identity verification providers)

PURPOSES FOR COLLECTING PERSONAL INFORMATION

We use your personal information to:

- Provide and maintain your accounts
- Process transactions
- Verify your identity
- Detect and prevent fraud
- Comply with legal obligations
- Improve our products and services

Use of Biometric Voice Verification

We may use voice recognition technology to:

- Verify your identity during phone or digital interactions
- Prevent fraud and unauthorized account access
- Improve authentication efficiency

Biometric data is:

- Used solely for authentication and security purposes
- Not sold or shared for marketing
- Retained only as long as necessary for verification and legal compliance

---

HOW WE SHARE YOUR PERSONAL INFORMATION

We may share your information with:

- Service providers (e.g., payment processors, identity verification vendors)
- Regulatory authorities and law enforcement (as required)
- Joint marketing partners (financial services only, where permitted)

We do NOT sell your personal information.

DATA RETENTION

We retain your personal information:

- As long as necessary to provide services
- As required by law or regulatory obligations
- Until you request deletion (subject to legal exceptions)

Biometric data (voiceprints) is retained only as long as needed for identity verification and fraud prevention.

YOUR CALIFORNIA PRIVACY RIGHTS

If you are a California resident, you have the following rights:

1. Right to Know

Request disclosure of:

- Categories of personal information collected
- Sources of data
- Business purposes
- Third parties with whom data is shared

2. Right to Access

Request a copy of your personal information

3. Right to Delete

Request deletion of your personal information (subject to legal exceptions)

4. Right to Correct

Request correction of inaccurate personal information

5. Right to Opt-Out of Sale or Sharing

FAST Credit Union does **not sell** personal information

6. Right to Limit Use of Sensitive Personal Information

You may request limits on use of:

- Biometric data (including voice data)
- Geolocation
- Account credentials

7. Right to Non-Discrimination

You will not be discriminated against for exercising your rights. Please note that without the use of certain Personal Information, we may not be able to provide (or continue providing) relevant products or services or otherwise do business with you. However, we will not discriminate against you for exercising any of your CCPA rights or deny you goods or services except as permitted by the CCPA or other applicable law.

HOW TO EXERCISE YOUR RIGHTS

You may submit requests:

- **Email:** membercenter@fastcu.com
- **Phone:** 559-584-0922
- **Mail:** FAST Credit Union, 312 W. 7th St., Hanford, Ca 93230
- **Online:** www.fastcu.com

We will verify your identity before processing your request, which may include authentication using account data or **voice verification (if applicable).**

CHILDREN'S PRIVACY

Our services are not directed to children under 13, and we do not knowingly collect their personal information. We have no actual knowledge of selling or sharing personal information of persons under 16 years old.

Automated Decision-Making Technology (ADMT) Disclosure

1. Overview

FAST Credit Union uses certain automated systems and technologies to process personal information and assist in providing financial services. These systems, sometimes referred to as Automated Decision-Making Technologies (ADMT), may include machine learning, data analysis, or artificial intelligence tools that help evaluate eligibility for products or detect potential fraud.

2. When We Use ADMT

We may use ADMT in connection with:

- Loan or credit application evaluation and decisioning;

- Identity verification and fraud prevention;

- Account monitoring for unusual activity or risk;

- Online banking or mobile app security functions; and

- Marketing and member engagement, such as personalized recommendations.

When we use ADMT to make or substantially assist a decision that has a significant effect on you—such as approving or denying a loan application—you will receive a notice before or at the time of use explaining the purpose and your related rights.

3. Consumer Rights

Under the California Consumer Privacy Act (CCPA/CPRA) and related CPPA regulations:

- Access: You may request information about how the Credit Union used ADMT in your case, including the general logic used and how it affected the decision.

- Opt-Out: You may opt out of the use of your personal information for certain types of automated decision-making or profiling, unless such processing is necessary for fraud prevention, security, or regulatory compliance.

- Human Review: If a significant decision was made or supported by ADMT, you may request a human review or appeal of that decision.

4. We ensure that all ADMT systems are regularly tested for accuracy, fairness, and bias, and that decisions are made in compliance with applicable federal and

state laws, including the Equal Credit Opportunity Act (ECOA) and Fair Credit Reporting Act (FCRA). The Credit Union reviews all ADMT tools at least annually as part of its risk and compliance programs.

USE OF GLIA VIRTUAL ASSISTANT (GVA)

The Glia Virtual Assistant is as Al-powered virtual assistant which replaces touch-tone, menu-based interactive voice response technology. This technology helps FAST members experience a reduction in wait times to resolve common issues. The Glia Virtual Assistant actively identifies when Human Assistance is necessary as well. All of this helps FAST improve resolution times and ultimately lower costs to its Members.

GVA collects information through use of Customer Sites, including:

Device Information - GVA collects information about devices running Customer Sites, including Internet protocol address, MAC address, browser type, operating system, and, if applicable, carrier information and country code.

Technical and Performance Data – GVA collects technical data through our Software Development Kits (SDK) and services to help diagnose issues, improve performance, and understand product usage. This may include SDK version, device type, feature usage, session events, and other non-personal system details used internally for product reliability and support.

Site Usage Information – GVA collects information about how Customer Sites are used, such as the frequency and duration of usage, and your activities on Customer Sites, such as browsing patterns, mouse movements, scroll movements and purchase history.

Information provided by you - GVA may collect information provided directly, such as contact details, feedback, chat transcripts (including text, audio, and video), and survey responses.

COOKIES & ONLINE TRACKING

We use cookies to:

- Enable website functionality
- Improve user experience
- Analyze website performance

We do not sell or share browsing data for advertising purposes.

SECURITY

We implement administrative, technical, and physical safeguards to protect your personal information, including:

- Encryption
- Secure systems
- Access controls

CHANGES TO THIS POLICY

We may update this Privacy Policy periodically. Updates will be posted on our website with a revised effective date.

CONTACT US

If you have questions about this Privacy Policy:

FAST Credit Union
312 W. 7th St.

Hanford, Ca 93230

Email: membercenter@fastcu.com
Phone: 559-584-0922

NOTICE AT COLLECTION (CCPA SHORT FORM)

We collect personal information, including biometric voice data, to provide financial services, verify identity, and prevent fraud. We do not sell your personal information. You have rights under California law to access, delete, and control your data.