GEORGIA'S OWN CREDIT UNION

Biometric Information Policy

Effective Date: July 1, 2026

Georgia's Own Credit Union is committed to protecting the privacy, confidentiality, and security of our members' personal information. This Biometric Information Policy describes generally how we collect, use, store, retain, disclose, and delete biometric information in connection with certain biometric authentication, security, and fraud prevention activities.

1. What Is Biometric Information

For purposes of this Policy, "Biometric Information" means information derived from an individual's unique biological, physical, or behavioral characteristics that can be used to identify that individual.

Biometric Information may include, by way of example:

- Voiceprints or voice recognition data
- Facial geometry or facial recognition data
- Fingerprints or fingerprint templates
- Hand or palm geometry
- Iris or retina recognition data
- Other biometric identifiers or information derived from the measurement, analysis, or conversion of physical or behavioral characteristics used for identification or authentication

Biometric Information does not include photographs, audio recordings, videos, usernames, passwords, PINs, or other personal information unless and until such data is processed or converted into a biometric identifier or biometric template used to identify a member by or on behalf of the Credit Union.

2. How Georgia's Own Credit Union Collects Biometric Information

Georgia's Own Credit Union collects Biometric Information when a member enrolls in biometric authentication services and, in certain cases, through security and fraud prevention systems used to protect accounts and transactions, as permitted by law.

Biometric Information may be collected through:

- Enrollment in biometric authentication for telephone, online, mobile, branch, ATM, or other service channels
- Member use of devices, applications, or platforms that support biometric based identity verification
- Security or fraud prevention systems, including tools that analyze biometric or behavioral characteristics and interaction patterns to help detect unauthorized or fraudulent activity
- Video surveillance and physical security systems that may capture images or, where enabled, generate, analyze, or compare biometric identifiers such as facial geometry or facial recognition data

Biometric Information may be collected using systems operated by Georgia's Own Credit Union or through technology provided by third party service providers acting on our behalf.

Enrollment in biometric services requires the member's knowledge, participation, and consent, where required by applicable law.

However, fraud prevention and security monitoring tools may automatically collect or analyze biometric or biometric-derived information as part of providing and securing services, as permitted by law and disclosed in this Policy and applicable privacy or digital banking disclosures and any other applicable notices provided at or prior to the point of collection, where required by law.

Use of Video and Security Systems

Georgia's Own Credit Union uses video surveillance systems in and around its facilities for security, safety, and fraud prevention purposes, including systems provided by third-party vendors.

These systems may include capabilities that analyze video or image data to detect, recognize, or compare facial characteristics or other biometric identifiers, whether in real time or retrospectively, if and when such capabilities are enabled.

If facial recognition or similar biometric identification technologies are enabled or used:

- Such use will be limited to legitimate security, fraud prevention, or investigative purposes
- The Credit Union will provide appropriate notice where required by law
- Any resulting biometric identifiers will be governed by this Policy to the extent applicable

The Credit Union does not use facial recognition technology for marketing, profiling, targeted advertising, or product eligibility decisions and does not sell or commercialize biometric data derived from such technologies.

The Credit Union may provide additional notice through signage or other disclosures in areas where video surveillance or biometric-enabled technologies are in use, as appropriate or required by law.

3. How Georgia's Own Credit Union Uses Biometric Information

Georgia's Own Credit Union uses Biometric Information solely for legitimate business purposes, including:

- Verifying a member's identity
- Authenticating access to accounts, services, or transactions
- Protecting members and the credit union against fraud, identity theft, and unauthorized access
- Enhancing the security and efficiency of member service interactions
- Supporting physical security investigations, incident response, and threat detection through video and access control systems, including those with biometric analysis capabilities
- Complying with applicable legal and regulatory requirements

This includes the use of behavioral biometrics and analytics tools to assess whether account or session activity is consistent with legitimate user behavior.

Biometric Information is not used to evaluate personal characteristics unrelated to identity verification and is not used for marketing, profiling, targeted advertising, or product eligibility decisions.

4. Storage and Security of Biometric Information

Georgia's Own Credit Union maintains reasonable administrative, technical, and physical safeguards designed to protect Biometric Information, including:

- Encryption of biometric data during transmission and storage, to the extent practicable
- Controls designed to prevent unauthorized access, disclosure, or use
- Access restrictions limited to authorized systems, personnel, and service providers
- Ongoing assessment of security practices and oversight of vendor controls

Where feasible and consistent with system design and security requirements, biometric templates are stored separately from other personal or account information.

Georgia's Own Credit Union treats biometric information as sensitive personal information and maintains administrative, technical, and physical safeguards consistent with applicable federal and state privacy and information security laws and regulatory guidance. Biometric information is handled as part of the Credit Union's written information security program and is subject to applicable risk assessment, access controls, monitoring, and incident response requirements. However, no administrative, technical, or physical safeguards can be guaranteed to be completely secure.

5. Disclosure and Sharing of Biometric Information

Georgia's Own Credit Union does not sell, lease, trade, or otherwise profit from Biometric Information.

Biometric Information may be disclosed only:

- To third party providers that provide biometric authentication, behavioral analytics, security, or fraud prevention services and that are contractually required to protect such information
- To third party service providers that provide cloud-based video surveillance, access control, or physical security systems, which may process video or image data and, where enabled, support biometric analysis capabilities
- To regulators, law enforcement, or governmental authorities when required by law, subpoena, court order, or similar legal process
- As otherwise permitted or required by applicable law

Any third party that stores, processes, or accesses Biometric Information on behalf of Georgia's Own Credit Union must maintain safeguards consistent with this Policy to the extent required by contract or applicable law.

6. Retention of Biometric Information

Georgia's Own Credit Union retains Biometric Information only for as long as reasonably necessary to fulfill the purposes for which it was collected, including to detect, investigate, or prevent security incidents, fraud, or illegal activity, unless a longer retention period is required or permitted by law.

For video and image data processed through security systems, retention periods may be based on system configurations, security needs, and vendor capabilities. If such data is used to generate biometric identifiers, those identifiers will be retained in accordance with this Policy and applicable law.

Factors considered in determining retention include:

- Continued participation in biometric enabled services
- Security, fraud prevention, and risk management needs
- Applicable regulatory or legal requirements
- Operational necessity

Biometric information is subject to Georgia's Own Credit Union's incident response and data breach notification procedures. In the event of a security incident involving biometric information, the Credit Union will assess, respond, and provide notifications as required by applicable federal and state law and regulatory guidance.

7. Deletion of Biometric Information

Biometric Information will be permanently deleted in accordance with applicable law and the Credit Union's records retention practices, including when:

- A member withdraws consent or opts out of biometric authentication, where applicable
- The biometric enabled service is discontinued
- The member relationship ends and there is no lawful, regulatory, or operational reason to retain the information
- The information is no longer necessary for its original, disclosed purpose

Deletion is performed using methods designed to render Biometric Information not reasonably retrievable, within a reasonable timeframe, subject to system capabilities and legal requirements.

Where biometric information or related video or image data is maintained by third party service providers, including security system providers, deletion will occur in accordance with applicable contracts, system configurations, and legal requirements, which may vary by provider.

8. Member Choice and Consent

Certain uses of Biometric Information, including biometric authentication services, are voluntary and require a member's knowledge, participation, and consent where required by applicable law.

However, the Credit Union also employs security and fraud prevention measures, including video surveillance, behavioral analytics, and related technologies, which may involve the collection or analysis of biometric or biometric-derived information as part of standard security operations necessary to protect accounts, facilities, employees, and members. These activities do not depend on individual enrollment and may not be disabled.

Members may:

- Decline to enroll in any biometric-enabled authentication services
- Use available non-biometric authentication methods
- Withdraw consent for enrolled biometric services and request deletion of Biometric Information, subject to applicable law and system limitations

Georgia's Own Credit Union provides commercially reasonable alternatives for account access. Certain security and fraud prevention measures may operate by default and may not be individually disabled. Choosing not to use biometric services or withdrawing consent will not prevent members from accessing accounts or services through available non-biometric authentication methods.

9. Changes to This Policy

Georgia's Own Credit Union may update this Biometric Information Policy from time to time to reflect changes in technology, law, regulatory guidance, or business practices. Updates will be posted on the Credit Union's website. The Credit Union will provide additional notice or obtain consent for material changes only to the extent required by applicable law.

10. Policy Scope and Limitations

This Biometric Information Policy is intended to describe Georgia's Own Credit Union's general practices regarding biometric information and to support compliance with applicable laws and regulatory guidance. This Policy is not intended to create, and does not create, any contractual, statutory, or other legal rights, obligations, or causes of action beyond those provided under applicable law.

This Policy applies only to Georgia's Own Credit Union's biometric information practices and does not represent compliance with the biometric privacy laws or regulations of jurisdictions outside Georgia unless expressly stated and is not intended to create obligations beyond those imposed by applicable law.

Nothing in this Policy is intended to expand any rights or obligations beyond those required under applicable law.