

# Privacy Notice for the California Consumer Privacy Act

## About This Notice

This notice describes your rights and how we collect, use, retain, and disclose the personal information of California residents (“you”) under the California Consumer Privacy Act of 2018 (CCPA). It supplements the information in our other privacy notices. This notice applies only to California residents and their personal information.

This notice is provided jointly by the organizations that make up Global (“we” or “us”), including:

- » Global Federal Credit Union;
- » Global Credit Union Home Loans, LLC (including dba Procura Mortgage Company); and
- » Global Credit Union Insurance Brokers, LLC (including dba Global CU Insurance Agency, LLC).

You may contact us with questions or concerns about this notice and our information practices by:

- » Emailing us at [memberservice@globalcu.org](mailto:memberservice@globalcu.org) or
- » Calling our Member Service Center at 800-525-9094.

Definitions provided in this notice may vary from definitions in other notices. For purposes of this notice:

- » **Personal information** means any information that is, or reasonably could be, linked to a particular individual or household. This information is divided into several categories under the CCPA.
- » **Sensitive personal information** means personal information that falls into certain special categories under the CCPA.
- » **Third party** means a person or company other than Global Federal Credit Union, our similarly branded affiliates, or our contractors or service providers.
- » **Sharing** means disclosure to a third party for purposes of cross-context behavioral advertising.
- » **Selling** means disclosure to a third party in exchange for anything of value.

The CCPA exempts from most of its requirements certain information, activities, or entities already protected by other laws. Much of the personal information we collect is already regulated by these or other laws. For example, the CCPA exempts:

- » Information subject to the requirements of the Gramm-Leach-Bliley Act (GLBA), which applies to most personal information collected while providing financial services for personal or household purposes;
- » Activities governed by the Fair Credit Reporting Act (FCRA), such as providing your personal information to credit reporting agencies or obtaining credit reports about you; and
- » Information subject to the Driver’s Privacy Protection Act.

We may change this notice from time to time. When we do, we will post the revised version on our websites with a new date.

## How We Secure Your Personal Information

Keeping your personal information secure and private is among our most important priorities. Consistent with our obligations under applicable laws and regulations, we maintain physical, technical, and organizational safeguards to protect your personal information against improper access, disclosure, alteration, retention, and destruction.

# Your Rights

Subject to some limitations, you have the right to:

- » Opt out of the sale and sharing of your personal information.
- » Know what information we have collected about you; the categories of sources from which we collect personal information; our purposes for collecting, sharing, or selling that information; and the categories of third parties to whom we disclose personal information.
- » Know what information we have sold or shared about you.
- » Obtain a copy of your personal information from us.
- » Request that we erase your personal information and direct those we've provided with your personal information to do the same.
- » Request that we correct personal information about you.
- » Be free from discrimination or retaliation for exercising your rights under the CCPA, including exercise of your rights as an employee, applicant, or independent contractor.

Within 10 days of receiving your request, we will acknowledge your request and provide information about how we will process the request.

We accept and process requests directly from you or from your authorized agent in the same manner, subject to verification of authorization as outlined below.

To verify your identity or to verify your representative's authorization to make a request on your behalf, we may request further information or action. If we cannot adequately verify your identity or your representative's authorization to submit a request on your behalf, we may decline all or part of a request. We will notify you of our decisions. Verification helps protect you from identity theft or other violations of your privacy. At our discretion, and depending on the risks posed by a request, we may ask that you verify access to your email address or phone number, provide documents to identify you or to demonstrate your authority to make a request on another individual's behalf, or make your request in person. If your authorized agent makes a request on your behalf, we may require that you identify yourself directly.

If we cannot complete your request within 45 days, we will notify you that we are extending the request and provide you with an explanation for the delay. We may take up to an additional 45 days, for a total of 90 days from the date you submit your request.

If your request is excessively difficult, we may reach out to you to gather more specific information about your request. If you make unfounded or excessive requests, we may decline them.

To exercise your rights to deletion, correction, or access to your personal information under the California Consumer Privacy Act, you can:

- » Visit [www.globalcu.org/privacy](http://www.globalcu.org/privacy) to submit a Privacy Rights Request;
- » Call our Member Service Center at 800-525-9094; or
- » Visit a Global branch.

You can opt out of the sale and sharing of your personal information by:

- » Setting your browser to send an Opt Out Preference Signal (also known as a Global Privacy Control) or
- » Visiting [www.globalcu.org/privacy](http://www.globalcu.org/privacy) or clicking the link on our website that says "Do Not Sell or Share My Personal Information."

# Global Information Practices

The specific personal information that we collect, use, retain, and disclose, and the purposes for disclosure, may vary depending on the relationship you have with Global, including the products or services you obtain from us.

## Why We Collect Your Personal Information

We use your personal information in many ways to operate, manage, and develop our business and to provide our products and services to you, including for the following:

- » Performing services, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services;
- » Securing our information systems, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;
- » Undertaking activities to verify or maintain the quality or safety of services controlled by us, and to improve, upgrade, or enhance the service controlled by the business;
- » Debugging to identify and repair errors that impair existing intended functionality;
- » Short-term, transient use where the information is not disclosed to a third party and is not used to build a profile or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction;
- » Marketing and advertising our products and services;
- » Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards;
- » Undertaking internal research for technological development and demonstration; and
- » Complying with laws and regulations and to comply with other legal process and law enforcement requirements (including any internal policy based on or reflecting legal or regulatory guidance, codes or opinions).

## Sources of Personal Information

We collect or have collected your personal information from sources that may include, depending on your relationship with Global:

- » You, your representatives, your family, and your business associates;
- » Service providers, contractors, and third parties;
- » Public records, including federal, state, and local government sources;
- » Our affiliates;
- » Social media; and
- » Our websites and mobile apps.

## Personal Information

We collect, use, and disclose personal information for a business purpose as follows, and have done so over the previous 12 months:

Categories of Personal Information	Business Purpose(s) for Disclosure	Categories of Third Parties/Service Providers We May Disclose To
Identifiers, such as name, government-issued identifiers such as Social Security number, account numbers, email address, or online identifiers such as Internet Protocol (IP) address.	<ul style="list-style-type: none"> <li>Account opening and servicing</li> <li>Customer support</li> <li>Information security</li> <li>Fraud prevention</li> <li>Legal compliance</li> <li>Advertising and marketing (including cross-context behavioral advertising)</li> </ul>	<ul style="list-style-type: none"> <li>Payment networks/processors</li> <li>Credit reporting agencies (as permitted)</li> <li>IT/Hosting vendors</li> <li>Fraud prevention service providers</li> <li>Government entities</li> <li>Advertising and marketing partners</li> <li>Affiliates</li> </ul>
Other records protected under California law, including insurance, medical, and financial information.	<ul style="list-style-type: none"> <li>Account servicing</li> <li>Product underwriting</li> <li>Claims processing</li> <li>Compliance and reporting</li> </ul>	<ul style="list-style-type: none"> <li>Payment networks/processors</li> <li>Insurance administrators</li> <li>Government entities</li> <li>Audit and compliance service providers</li> <li>Affiliates</li> </ul>
Characteristics of protected classifications under California or federal law, such as sex and marital status.	<ul style="list-style-type: none"> <li>Compliance with equal opportunity laws in lending and employment</li> <li>Fair lending analytics</li> </ul>	<ul style="list-style-type: none"> <li>Government entities</li> <li>Audit and compliance service providers</li> <li>Affiliates</li> </ul>
Commercial information, such as transaction information and purchase history.	<ul style="list-style-type: none"> <li>Account servicing</li> <li>Fraud monitoring</li> <li>Analytics</li> <li>Regulatory reporting</li> </ul>	<ul style="list-style-type: none"> <li>Payment networks/processors</li> <li>Credit reporting agencies (as permitted)</li> <li>Fraud prevention service providers</li> <li>Data analytics service providers</li> <li>Government entities</li> <li>Affiliates</li> </ul>
Biometric information, such as voice recordings or behavioral characteristics.	<ul style="list-style-type: none"> <li>Identity verification</li> <li>Fraud prevention</li> <li>Service quality</li> <li>Dispute resolution</li> <li>Branch/ATM security</li> </ul>	<ul style="list-style-type: none"> <li>Security vendors</li> <li>Fraud prevention service providers</li> <li>Contact center recording/quality vendors</li> <li>Government entities</li> <li>Affiliates</li> </ul>
Internet or network activity information, such as browsing history.	<ul style="list-style-type: none"> <li>Security and debugging</li> <li>Website/App performance</li> <li>Advertising and marketing (including cross-context behavioral advertising)</li> <li>Analytics</li> </ul>	<ul style="list-style-type: none"> <li>IT/Hosting/CDN providers</li> <li>Advertising and marketing partners</li> <li>Data analytics service providers</li> <li>Government entities</li> </ul>
Geolocation data, such as device location and IP address location.	<ul style="list-style-type: none"> <li>Security and fraud prevention</li> <li>Transaction integrity</li> <li>Advertising and marketing (including cross-context behavioral advertising)</li> </ul>	<ul style="list-style-type: none"> <li>Fraud prevention service providers</li> <li>Payment networks/processors</li> <li>Advertising and marketing partners</li> <li>Data analytics service providers</li> <li>Government entities</li> </ul>
Audio, electronic, visual, and similar information, such as call and video recordings.	<ul style="list-style-type: none"> <li>Branch/ATM security</li> <li>Service quality</li> <li>Dispute resolution</li> <li>Legal compliance</li> </ul>	<ul style="list-style-type: none"> <li>Security vendors</li> <li>Fraud prevention service providers</li> <li>Contact center recording/quality vendors</li> <li>Government entities</li> <li>Affiliates</li> </ul>

## Personal Information (continued)

Categories of Personal Information	Business Purpose(s) for Disclosure	Categories of Third Parties/Service Providers We May Disclose To
Professional or employment-related information, such as work history and prior employer.	<ul style="list-style-type: none"> <li>• Product underwriting</li> <li>• Employment applications</li> <li>• Legal compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Background screening/verification vendors</li> <li>• Government entities</li> </ul>
Education information, such as student records and directory information.	<ul style="list-style-type: none"> <li>• Product underwriting</li> <li>• Employment applications</li> <li>• Discounts/Benefits verification</li> </ul>	<ul style="list-style-type: none"> <li>• Background screening/verification vendors</li> <li>• Government entities</li> </ul>

## Sensitive Personal Information

Global uses sensitive information only for purposes which are not subject to the right to limit under the CCPA and applicable regulations. We collect, use, and disclose your information for a business purpose as follows, and have done so over the previous 12 months:

Categories of Sensitive Personal Information	Business Purpose(s) for Disclosure	Categories of Third Parties/Service Providers We May Disclose To
Social Security, driver's license, state identification card, or passport number.	<ul style="list-style-type: none"> <li>• Identity verification</li> <li>• Tax reporting</li> <li>• Product underwriting</li> <li>• Fraud prevention</li> <li>• Legal compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Underwriting/Verification vendors</li> <li>• Tax reporting/statement processors</li> <li>• Government entities</li> <li>• Affiliates</li> </ul>
Account access information such as username, or financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.	<ul style="list-style-type: none"> <li>• Provision of debit/credit card services</li> <li>• Online/Mobile account access</li> <li>• Authentication and fraud prevention</li> </ul>	<ul style="list-style-type: none"> <li>• Payment networks/processors</li> <li>• Card issuers</li> <li>• Authentication/Fraud service providers</li> <li>• Government entities</li> </ul>
Precise geolocation (within the area of a circle with a radius of 1,850 feet).	<ul style="list-style-type: none"> <li>• Delivery of electronic services</li> <li>• Fraud/Security</li> <li>• Branch/ATM access controls</li> </ul>	<ul style="list-style-type: none"> <li>• Security vendors</li> <li>• IT/Hosting/Mobile SDK providers</li> <li>• Government entities</li> </ul>
Racial or ethnic origin, religious or philosophical beliefs, or union membership.	<ul style="list-style-type: none"> <li>• Compliance with equal opportunity laws in lending and employment</li> <li>• Fair lending analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Audit and compliance service providers</li> <li>• Government entities</li> </ul>
The contents of messages (such as letters, email, or text) except where we are the intended recipient of the communication.	<ul style="list-style-type: none"> <li>• Handling complaints/disputes</li> <li>• Compliance and legal process.</li> </ul>	<ul style="list-style-type: none"> <li>• Legal counsel/eDiscovery providers</li> <li>• Government entities</li> </ul>
The processing of biometric information for the purpose of unique identification.	<ul style="list-style-type: none"> <li>• Authentication</li> <li>• Fraud prevention</li> <li>• Service-quality analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Security vendors</li> <li>• Fraud prevention service providers</li> <li>• Contact center analytics providers</li> <li>• Government entities</li> </ul>
Information collected and analyzed concerning health (Employees Only).	<ul style="list-style-type: none"> <li>• Provision and administration of employee health benefits</li> <li>• Compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Health insurance carriers</li> <li>• Benefit administrators</li> <li>• Government entities</li> </ul>

## Sensitive Personal Information (continued)

Information collected and analyzed concerning sex life or sexual orientation (Employees Only).

- Provision and administration of employee health benefits
- Compliance

- Health insurance carriers
- Benefit administrators
- Government entities

## Retention Periods

For each of the categories of personal information and sensitive personal information above, we retain the information according to our retention policies for as long as necessary:

- » To provide our products, services, or benefits to you;
- » For compliance and legal purposes;
- » For security and fraud prevention purposes;
- » To facilitate resolution of credit and transaction disputes;
- » To market, maintain, and improve products and services;
- » To maintain and improve systems, operations, and facilities;
- » To develop new products and services; and
- » For other purposes compatible with the purposes and context of collection.

Retention periods vary by the type of transaction, interaction, or relationship for which the personal information was collected.

## Third-Party Disclosure, Sharing, and Selling

We may disclose your personal information to the following categories of third parties:

- » Businesses which provide us with services related to digital marketing, including infrastructure, ad placement, and analysis; and
- » Government entities as required or permitted by laws or regulations.

If you are 16 years old or older, we can sell or share your personal information unless you opt out. However, if we know that you are less than 16 years old, we must obtain consent to share or sell your information. If you are 13-15, you can provide consent. If you are under 13, your parent or guardian can provide consent.

We share your personal information for purposes of cross-context behavioral advertising unless you tell us not to or we know you are less than 16 years old in the context of sharing. We do not knowingly share the personal information of individuals less than 16 years old. We share this information with third parties who place ads or help us optimize ad placement. The information we share is focused on improving the relevance of the advertising you see, for example to avoid advertising services to you that you already receive from us.

To the extent that sharing for purposes of cross-context behavioral advertising also constitutes selling as defined by the CCPA, we sell your personal information. However, we will never disclose your personal information in exchange for money. We disclose your personal information under these circumstances only to improve the relevance of the behavioral advertising you receive and measure its effectiveness.

In the past 12 months, we have shared or sold the following categories of personal information:

- » Identifiers, including your name, phone number, email address, and IP address;
- » Network activity, such as the fact that you visited our website; and
- » Geolocation, including country and ZIP code.