Summit Credit Union Privacy Notice

Effective Date: May 28, 2026

WE RESERVE THE RIGHT TO CHANGE THIS PRIVACY NOTICE FROM TIME TO TIME, AND IT IS YOUR RESPONSIBILITY TO ENSURE THAT YOU AGREE TO THESE TERMS PRIOR TO USING OUR WEBSITE(S) OR PROVIDING INFORMATION TO US.

Overview

Summit Credit Union ("Summit," "we," "us," or "our") is a Wisconsin-chartered credit union with an open charter, serving members primarily in Wisconsin, with some members in other states and internationally through our relationship with the World Council of Credit Unions. Summit is committed to protecting your personal information and privacy. This Privacy Notice explains how we collect, use, share, and safeguard your personal information when you use this website (https://www.summitcreditunion.com or "Website"), our mobile application(s), and rewards programs. For information about how and why we collect, use, and share your non-public financial information, please visit our Financial Privacy Notice.

This website may contain links to third-party websites. Summit Credit Union does not control and is not responsible for the data handling practices or content of those websites. We encourage you to review their privacy policies and privacy notices.

Please read this Privacy Notice carefully to understand our policies and practices regarding your personal information. When you interact with us or provide us with your personal information, you agree to our collection, use, and sharing of it as described in this Privacy Notice.

This Notice may change from time to time (see Changes to this Privacy Notice below). Your continued use of this Website, our mobile application(s), or our rewards programs after we make changes as described here is acceptance of those changes, so please check here periodically for updates.

This Privacy Notice governs our handling of personal and other information that does not qualify as non-public personal information ("NPI") under the Gramm-Leach-Bliley Act ("GLBA"). Our separate Financial Privacy Notice ("Financial Privacy Notice") governs how we collect, use, and share NPI about our members in connection with providing financial products and services, including our digital banking platform. The Financial Privacy Notice supplements this Privacy Notice.

1. Applicability of this Privacy Notice

This Notice applies to information collected from:

- members and account holders
- Website visitors
- users of our mobile applications (including Summit Credit Union app, SCU Business app)
- users of our digital banking platform
- users of our rewards portals (Summit Cash Perks, Razr Rewards); and
- prospective members and others who interact with us online.

If you are a California resident, please see the "SUPPLEMENTAL PRIVACY NOTICE FOR CALIFORNIA RESIDENTS ("CALIFORNIA PRIVACY NOTICE")" below.

Personal information collected, processed, or disclosed in connection with Summit's provision of financial products or services to its members is governed by federal financial privacy laws, including the GLBA, and is addressed in our separate Financial Privacy Notice. If you are a resident of California, the California Financial Information Privacy Act also applies.

2. Sources of Personal Information ("PI")

We collect personal information directly from you, and from sources such as advertising networks, You might provide the following categories of personal information to us when you enter data into applications apply or register for our products and services, or otherwise disclose it to Summit Credit Union, whether electronically or in person, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

We collect the following categories of information:

A. Information You Provide Directly

- name, mailing address, phone number, and/or email address
- government-issued identification (for KYC/identity verification)
- date of birth, tax identification number, and other identifiers
- account credentials (username, encrypted password)
- account and transaction information (account numbers, balances, rewards balances, transaction data)
- biometric data (such as Face ID, photo ID comparison, fingerprinting) for fraud prevention, authentication, and identity verification
- names, email address, and/or phone number of payment recipients and senders (for payment features such as Zelle)
- purchase history information (from Summit transactions and partner merchants); and
- other information you provide when registering or applying for products or services and when communicating with us.

B. Information Collected Automatically

Each time you visit this Website, our web servers might automatically collect the following information:

- technical information such as device and browser information (IP address, device ID, operating system, browser plug-in type, and version)
- geolocation data (city/state or zip code only) (for ATM/branch locator, address autofill, and certain digital banking features)
- Website or mobile app usage data (via cookies, pixels, tags and analytics software tools such as Google Analytics and Microsoft Clarity)
- "session" data, clickstream data, and usage logs
- member engagement data (such as interactions with our digital banking platform or rewards programs). For information about how we use, disclose, and protect data collected through the digital banking platform, please see our Financial Privacy Notice.

C. Information Provided by or Collected from Third Parties

We obtain information about you from the following categories of third parties:

- payment processors and financial partners (for transaction settlement)
- compliance and fraud prevention vendors (e.g., Alloy, BioCatch)
- marketing and analytics service providers
- partner merchants (for rewards/incentive program participation)
- data brokers and marketing data providers (for marketing targeting and audience development)

We do not intentionally collect information from children under 13. See the "Children's Privacy" section below.

3. How We Use Your Information

We use your information to:

- provide, operate, and manage your accounts and services
- process transactions and rewards
- administer and manage rewards and incentive programs, including eligibility, redemption, and related communications
- authenticate your identity and secure your accounts (including biometric authentication)
- communicate with you about your accounts, and our products and services
- send you marketing and promotional communications
- allow you to participate in surveys, sweepstakes, contests, and/or similar promotions (unless you opt out)
- analyze and improve our products, services, mobile app(s), and website(s)
- detect, investigate, and prevent fraud or security incidents
- comply with legal, regulatory, and contractual obligations, including Anti- Money Laundering ("AML") and Know Your Customer ("KYC") requirements
- fulfill any other purpose disclosed to you at the time of collection or with your consent

We may use de-identified or aggregated data for analytics, product development, and lawful business purposes. We do not use automated processing (that is, processing without human review) of your personal information to make decisions that produce legal or similarly significant effects concerning you. We may use automated tools, such as analytics software, to analyze usage patterns and improve our services and communications, but we do not use this analysis to make decisions that produce legal or similarly significant effects concerning individual members.

We do not use or disclose sensitive personal information ("SPI") for purposes other than those allowed by applicable law.

4. Cookies and Tracking Technologies

Like many other companies, we and third-party partners use cookies, pixels, tags, scripts, and other tracking technologies (collectively, "Cookies"). Cookies are small files of information that are stored by your web browser on your computer, mobile or other device (e.g., tablet). These technologies help us:

- enable secure login and session management
- analyze and improve how users interact with our digital services
- support marketing and advertising efforts
- prevent fraud and protect our members

Some Cookies are set by us, while others are set by third-party providers. These include:

- Analytics providers, such as Google Analytics and Microsoft Clarity, which help us understand how visitors use our Website and mobile apps and improve our digital services; and
- Advertising and retargeting partners, such as Trade Desk, Google Ads, and Meta, which use pixels and similar technologies to collect information about your visits to our Website (such as your IP address, device identifiers, browsing behavior, and interactions with our content) in order to deliver relevant advertisements to you on third-party websites and platforms, measure the effectiveness of our advertising campaigns, and build audience segments.

Information collected by these third-party technologies may be transmitted to and stored by these third parties in the United States and is subject to their respective privacy policies.

Targeted Advertising and Retargeting

We work with third-party advertising partners, including Trade Desk, Google Ads, and Meta, who place pixels and similar tracking technologies on our Website. These technologies allow our advertising partners to recognize your device across different websites and platforms and to show you advertisements for Summit Credit Union's products and services based on your prior visits to our Website. This practice is sometimes referred to as "retargeting" or "remarketing."

The information collected through these pixels may include pseudonymous identifiers, cookie and device identifiers, mobile advertising identifiers, IP addresses, and information about your interactions with our Website. Our advertising partners use this information to personalize and deliver ads across devices, limit how often you see the same ad, measure the effectiveness of advertising campaigns, and attribute your actions (such as submitting an application) to specific ads.

California residents have the right to opt out of the "sharing" of personal information for cross context behavioral advertising purposes. Please see the California Privacy Notice below for more information.

You may also opt out of certain advertising partner practices directly:

- Trade Desk: visit the Network Advertising Initiative opt-out page at optout.networkadvertising.org
- Google Ads: visit Google Ads Settings at adssettings.google.com
- Meta: visit Meta's Ad Preferences at facebook.com/ads/preferences

Your Choices

You can manage your Cookie preferences at any time by using our Cookie Management Tool, powered by Osano, which allows you to 'Accept All,' 'Reject All,' or 'Manage Preferences' for cookies and tracking technologies, except those that are strictly necessary for this Website and services to function: **Manage Consent.**

You may also:

- block Cookies by changing your browser settings. Please note that blocking all Cookies may impact the functionality of this Website and digital services.
- opt-out of Cookies set by Google by visiting Google Ads Settings.
- learn more about Cookies and how to manage them at https://www.AboutCookies.org or https://allaboutcookies.org.
- enable a recognized Global Privacy Control (GPC) signal in your browser to communicate your privacy preferences. Our web servers will honor such signals, as required by law. For more information, please see the Do Not Track Signals section below.

You can also see which entities have currently enabled Cookies for your browser or mobile device and understand how to opt out of some of those Cookies, by accessing the Network Advertising Initiative's website at optout.networkadvertising.org or the Digital Advertising Alliance's website at optout.aboutads.info. Please note that these opt-out mechanisms are specific to the device or browser on which they are used. Therefore, you will need to opt out on every browser and device that you use.

Do Not Track Signals

Some internet browsers incorporate a "Do Not Track" ("DNT") feature that sends signals to websites you visit that you do not want to have your device's online activity tracked. Because there is not a uniform standard for how DNT signals are interpreted, this Website does not currently respond to DNT signals.

However, as explained above, this Website does recognize and honor the Global Privacy Control ("GPC") signal, as required by applicable law. If you use a browser or extension that sends a GPC signal, we will treat that as a valid request to opt out of the sale or sharing of your personal information, as described in this Privacy Notice.

Analytics Tools

We use third party software tools, such as Google Analytics and Microsoft Clarity, to help us understand Website and mobile app usage across devices, compile reports, and improve our digital services. These tools might collect information such as your device's IP address, other information about the device, and Website usage patterns. These tools also allow us to manage our digital services and collect information about your visit to our Website. Information collected by these third-party software tools might be transmitted to and stored by these third parties, which are based in the United States, and is subject to their privacy policies.

To learn more about Google Analytics' data practices and how to opt out, visit Google Analytics Opt-Out.

You may opt out of Microsoft Clarity analytics through our Cookie Management Tool by rejecting or disabling analytics cookies. If you previously consented, you may update your preferences at any time through the same tool.

Cookie Consent Management

We use a cookie consent management platform to manage cookie preferences on this Website. You can adjust your preferences at any time using the cookie management tool available here: **Manage Consent.**

5. Third Party Security Checks

To protect your personal information, including your financial information, we sometimes use tools and services provided by third parties to help us decide whether to accept data submissions from personal computers, mobile phones, or other devices. Third-party software and services might check whether user devices have been associated with fraudulent or abusive transactions in the past, such as reported instances of identity theft, account takeovers, or malware attacks. For this purpose, a Cookie, flash storage token, or other code file might be placed on your device to identify it in the future when your device visits this Website or connects with our other online or mobile applications. If you set your browser or device to reject these Cookies or tokens, you might not be able to access some features of our Website or other online applications.

When you access this Website or other online applications, we will transmit a third- party device identification code to the third-party provider, along with data concerning certain technical attributes of your device such as the model, operating system, and browser version, as well as the IP address (all of which are used to confirm device identification). We will then receive information from these third-party providers indicating that submissions from a user's device should not be accepted. We will also inform such third-party providers if we determine that a device has been used in connection with a fraudulent or abusive transaction with us. Finally, in certain situations, we will share with one or more of these third-party providers certain personal information and information about the device you are using.

If you receive a message from us indicating that your submission has not been processed, we will provide customer service contact information.

6. How and Why We Share Your Information

We share your personal information as follows:

- With service providers (e.g., Lumin, WithClutch, Alloy, BioCatch, Visa DPS, Velera, fingerprint.js): for payment processing, digital banking, analytics, fraud prevention, marketing, and other business operations
- With other financial institutions: for jointly marketing products and services
- With rewards software platform providers (e.g., Amplifi, Razr) and digital banking/loan origination vendors (e.g., Lumin, WithClutch): for rewards program processing
- With service providers: to help us comply with applicable laws and regulations, such as AML/KYC regulations
- With successors or assigns: in connection with a merger, reorganization, or similar transaction
- With legal or regulatory authorities: As required by law, regulation, subpoena, or legal process
- With your consent or at your direction: for software integrations or services, with your prior consent

For a list of the types of third parties with whom we share PI, please see the SUPPLEMENTAL PRIVACY NOTICE FOR CALIFORNIA RESIDENTS ("CALIFORNIA PRIVACY NOTICE") below.

For a list of the types of third parties with whom we share non-public personal information (NPI), please see our separate Financial Privacy Notice, which governs how we collect, use, and share such information about our members in connection with providing financial products and services.

To the extent we offer financial incentive programs (such as rewards programs, sweepstakes, or similar promotions) that involve the collection or use of personal information as consideration for participation, we will provide California residents with a separate Notice of Financial Incentive as required by the CCPA/CPRA. Note that to the extent such programs involve your personal financial information governed by the GLBA, that information is exempt from the CCPA's Notice of Financial Incentive requirement.

7. Links to Third Party Websites

This Website may contain links to third- party websites. Although these links were established to provide you with access to useful information, Summit Credit Union does not control and is not responsible for any of these websites or their content. We do not know or control what information third- party websites might collect and it might include personal information.

Summit Credit Union provides these links to you only as a convenience, and Summit Credit Union does not endorse or make any representations about using such third-party websites or any information, software or other products or materials found there, or any results that may be obtained from using them. We encourage you to review the privacy policies of websites you choose to link to from the Summit Credit Union Website so that you can understand how those websites collect, use, and share your information. Summit Credit Union is not responsible for the security or privacy practices of the linked websites.

8. Your Rights and Choices (Subject to Applicable Law)

- Right to Know (categories and specific pieces of personal information collected)
- Right to Delete
- Right to Correct inaccurate personal information
- Right to Opt-Out of Sale or Sharing of personal information
- Right to Limit Use and Disclosure of Sensitive Personal Information
- Right to Non-Discrimination for exercising any of the above rights
- Right to Opt-Out of Automated Decision-Making (to the extent applicable)

To exercise one or more of these rights with respect to your personal information, please see the "Contact Us" section below. After you submit a request, we will ask you for verify your identity and we will respond within statutory timeframes. Please also note that:

- some rights are limited by law or by our need to maintain certain records; and
- personal information we collect in connection with providing financial products or services is generally exempt from certain state privacy laws, including the California Consumer Privacy Act (CCPA/CPRA), and instead is subject to federal law.

Marketing and Communications: you can opt out of receiving promotional communications at any time by clicking the unsubscribe link in any marketing email we send you or by contacting us as described in the 'How to Contact Us' section below. Please note that we currently use SMS text messaging only for authentication and account-related alerts (such as past-due notices), and not for marketing purposes. If this changes in the future, we will provide you with an opportunity to opt out of marketing text messages at that time by replying "STOP."

Cookies and Tracking: You can adjust your preferences through your browser or device settings. Please see the "Cookies and Tracking Technologies" section above for more information.

9. Data Security

We use industry-standard security measures, including encryption, access controls, and secure facilities, to protect your personal information. We also regularly conduct due diligence and execute data processing agreements with our service providers and contractually require them to implement appropriate data security standards. However, no system is 100% secure; please protect your account credentials and promptly notify us of any suspected unauthorized activity.

To the extent we collect biometric data (such as facial recognition data used for Face ID authentication) or behavioral biometric data (such as device behavior patterns used for fraud detection), such data is collected and stored by our third-party vendors (including BioCatch, Alloy, and fingerprint.js) on their servers and/or in secure cloud environments (including Splunk and Snowflake). Such data is encrypted, is not shared with unauthorized third parties, and is accessible only on a need-to-know basis. We require our vendors to maintain appropriate security standards for all such data.

Access to your personal information is restricted to our employees, service providers and partners as described in this Privacy Notice.

10. Data Retention

We retain your information while your account is active, as needed to provide services, or as required by law and our record retention policies. When information is no longer needed, we securely delete or de-identify it.

11. Children's Privacy

Our Website and services are intended solely for users aged 13 and older. We do not direct our content, services, or marketing to children under 13 and we do not knowingly collect personal information from children under the age of 13. If we become aware that a user is under 13 and that personal information has been collected, we will promptly delete such information.

If you are a parent or guardian and believe your child has provided us with personal information, please Contact Us. We will verify your request and promptly delete the information.

12. International Data Transfers

Your information is stored and processed in the United States. We do not transfer your information outside the U.S.

13. Notice to Nevada Residents

In addition to California, certain states such as Nevada allow residents to opt out of the sale of certain types of personal information. Although we do not currently "sell" personal information as defined under these laws, we do share personal information as described in this Privacy Notice. You can Contact Us to submit a verified request to opt out of sales, and we will record your instructions and incorporate them in the future if our policy changes.

14. Changes to this Privacy Notice

Our business operations may change from time to time. As a result, it may be necessary for us to update or modify this Privacy Notice. We reserve the right to do so at any time. When we update this notice, we will revise the "Effective Date" at the top.

For material changes, such as expanding how we use or share your personal information, we will provide you with prominent notice (for example, by posting a prominent notice on this Website, sending you an email, or through other appropriate means) before those changes take effect.

For non-material changes and if you are not a member of Summit Credit Union, we will update the "Last Updated" date at the top of this notice and post the revised notice here.

If you have an existing relationship with us, we may also provide notice through your account or by otherwise using your contact information.

We encourage you to review this Privacy Notice periodically to stay informed about our information practices. Your continued use of this Website and our mobile apps after any changes become effective constitutes your acceptance of those changes.

15. Accessibility

We are committed to ensuring this Privacy Notice is accessible to individuals with disabilities. If you wish to access this Privacy Notice in an alternative format, please contact us as described below.

16. How To Contact Us

If you have any questions or concerns about this Privacy Notice, to exercise any of your rights described in the Your Rights and Choices section above, or to review or update your contact information, such as your email address, mailing address or telephone number, please contact us:

By email: memberservice@summitcreditunion.com
By postal mail, in person or telephone:
1709 Landmark Drive
Cottage Grove, WI 53527
(800) 236-5560

SUPPLEMENTAL PRIVACY NOTICE FOR CALIFORNIA RESIDENTS ("CALIFORNIA PRIVACY NOTICE")

For California residents, and to the extent the California Consumer Privacy Act (CCPA/CPRA) applies to personal information not subject to the GLBA (such as information collected from Website visitors, job applicants, or marketing contacts), this California Notice at Collection supplements this Privacy Notice.

The categories of personal information we collect, the purposes for which we use this information, and our retention practices are described below. We do not "sell" personal information for monetary consideration, but we might share certain online identifiers (such as IP addresses or device information) with analytics providers, such as Google Analytics and Microsoft Clarity, to help us understand how our Website and mobile applications are used and to improve our digital services. We also share certain online identifiers and browsing activity with advertising partners (such as Trade Desk, Google Ads, and Meta) for targeted advertising and retargeting purposes. California residents can opt out of these practices by clicking on the "Do Not Sell or Share My Personal Information" link at the bottom of this Website.

We retain personal information only as long as necessary to fulfill the purposes for which it is collected, as described in the Data Retention section in this Privacy Notice or as otherwise required by law. If we cannot specify an exact retention period for a category of personal information, we use criteria such as the type of information, our legal and regulatory obligations, and our business needs to determine how long we retain it.

Summary of Categories Collected and Retention Criteria:

Category of Personal Information (PI) or Sensitive Personal Information (SPI)	**Purpose of Collection**	**Retention Period/Criteria**	**Is Such PI Sold or Shared?**	**Categories of Third Parties with Whom PI or SPI is Shared**
Identifiers (PI) (e.g., name, email address, telephone number, mailing address, account credentials, IP address)	– Account setup and management – Communicating with Website visitors and credit union members – Security/ authentication – Marketing – Compliance (KYC/AML)	For as long as required by law/regulation (e.g., banking/KYC retention rules) or as needed for active accounts and services.	Not Sold. Shared.	Analytics providers; identity verification providers; advertising and marketing partners; digital banking and technology providers; payment processors and financial partners; and compliance and KYC/AML service providers
Internet or Other Electronic Network Activity (PI) (e.g., browsing history, interactions with Website or app, cookies,	- Website/app functionality - Security/fraud prevention - Analytics and service improvement - Targeted advertising	Retained in identifiable form only as long as necessary to support analytics, security, and client reporting; then deidentified	Not Sold. Shared.	Analytic providers; advertising and retargeting partners; fraud prevention and device intelligence

device/browser info, analytics data)		or deleted, unless a longer period is required by law.		vendors; and technology service providers supporting website and mobile application functionality.
Geolocation Data (SPI) (e.g., city, state, zip code, location for ATM/branch locator)	- Providing location-based services (e.g., ATM/branch locator) - Security/fraud prevention	Retained as long as necessary for the purpose collected or as required by law.	Not Sold. Shared.	Fraud prevention and security vendors; analytics providers; and technology and digital platform service providers.
Commercial Information (PI) (e.g., transaction and rewards data, purchase history)	- Account servicing - Rewards/incentive program administration - Compliance/audit - Analytics/product development	For as long as required by law/regulation or as needed for active accounts and services.	Not Sold. Shared.	Rewards and incentive program partners; payment processors and financial partners; analytics and product development service providers; marketing partners and merchants; and audit, legal, and compliance service providers.
Biometric Information (SPI) (e.g., facial images, Face ID, photo for ID verification)	- Security/authentication - Fraud prevention - Identity verification	Retained as long as necessary for authentication and security purposes, or as required by law.	Not Sold. Shared.	Identity verification providers; fraud prevention and behavioral analytics vendors; device intelligence providers; and secure cloud and infrastructure providers supporting these services.
Government Identifiers (SPI) (e.g., driver's license, passport, tax identification number)	- Identity verification (KYC/AML) - Compliance with legal obligations	For as long as required by law/regulation (e.g., KYC/AML retention rules).	Not Sold. Shared.	Analytic providers; Identity verification providers; compliance and KYC/AML service providers; fraud prevention vendors; and legal

				or regulatory authorities, as required by law.
Inferences (PI) (e.g., preferences/interests derived from interactions)	- Service improvement - Personalization - Marketing (if applicable)	Retained in identifiable form only as long as necessary for services, analytics, or marketing, then de-identified or deleted.	Not Sold. Shared.	Analytics providers; advertising and marketing partners; technology service providers supporting personalization; and data analytics and audience segmentation providers.

If you have questions about our data practices or your rights under California law, please see the Contact Us section.