NOTICE AT COLLECTION OF PERSONAL INFORMATION

1st United Credit Union (together with its subsidiaries and affiliates, also referred to as "we," "us," or "our" herein) is providing this notice pursuant to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA"). Any terms defined in the CCPA have the same meaning when used in this notice. This notice provides a summary of how we collect, use and share your personal information. We encourage you to read our Consumer Privacy Policy, which is available online at 1stunitedcu.org/privacy.

Application of this Notice

This notice applies to natural residents of the State of California from whom we collect personal information in the course of their acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of 1st United Credit Union.

Below are the categories of personal information we collect and the purposes for which we intend to use this information.

Categories Information We Collect

We will collect the following categories of personal information (which may overlap):

Category	Examples
A. Identifiers	A real name or alias; postal address; signature; home phone number or mobile phone number; bank account number, credit card number, debit card number, or other financial information; physical characteristics or description; email address; account name; Social Security number; driver's license number or state identification card number; or other similar identifiers.
B. Personal information categories described in Cal. Civ. Code § 1798.80(e)	Signature; state identification card number; physical characteristics or description; insurance policy number; education; employment or employment history; bank account number, credit card number, debt card number, or any other financial information; or medical information or health insurance information.
C. Protected classification characteristics under state 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, or veteran or military status.
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
E. Biometric information	Facial recognition, fingerprints, iris or retina scans, keystroke, or other physical patterns.
F. Internet or other similar network activity	Search history, browsing history, login information, and IP addresses on our information systems and networks.
G. Geolocation data	Time and physical location related to use of an internet website, application, device, or physical access to our office or branch locations.

H. Sensory data	Audio, electronic, visual or similar information collected on our monitoring and surveillance systems.
I. Professional or employment-related information.	Current or past job history, performance evaluations, disciplinary records, workplace injury records, disability accommodations, and complaint records; Emergency contact information, such as the name, phone number, address and email address of another person in the context of having an emergency contact on file; Personal information necessary for us to collect and retain to administer benefits for you and another personal relating to you (e.g., your spouse, domestic partner, and dependents), such as their name, Social Security Number, date of birth, telephone number, email, and address.
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Educational records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.
K. Inferences drawn from other personal information.	Profile reflecting a person's preference, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
L. Sensitive Personal Information.	A consumer's social security, driver's license, state identification card, or passport number; A consumer's account log-in, 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; A consumer's precise geolocation; A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; A consumer's genetic data; The processing of biometric information for the purpose of uniquely identifying a consumer; Personal information collected and analyzed concerning a consumer's health; and Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Personal information for purposes of the CCPA does not include:

- Publicly available information.
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, like personal information covered by certain financial sector laws, such as the Fair Credit Reporting Act (FRCA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA).

Use of Personal Information

We may use or disclose the personal information we collect to:

- To comply with all applicable laws and regulations.
- Recruit and evaluate job applicants and candidates for employment.
- Conduct background checks.
- Manage your employment relationship with us, including for:

    - Onboarding processes;
    - Timekeeping, payroll, and expense report administration;
    - Employee benefits administration;
    - Employee training and development requirements;
    - The creation, maintenance, and security of your online employee accounts;
    - Reaching your emergency contacts when needed, such as when you are not reachable or are injured or ill;
    - Worker's compensation claims management;
    - Employee job performance, including goals and performance reviewed, promotions, discipline, and termination; and
    - Other human resources purposes.
- Manage and monitor employee access to company facilities, equipment, and systems.
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential breaches of our policies and procedures.
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions.
- To prevent, detect and investigate security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and prosecute those responsible for that activity.
- Maintain commercial insurance policies and coverages, including for worker's compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- As necessary or appropriate to protect the rights, property or safety of us, consumers or others.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- Exercise or defend our legal rights and that of our employees, affiliates, customers, contractors, and agents.
- For client marketing purposes.

Selling or Sharing Personal Information

We will not sell your personal information.

Sharing Personal Information for Cross-Context Behavioral Advertising

Cross-context behavioral advertising refers to the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts.

We will not share your personal information for cross-context behavioral advertising purposes.

Retention of Personal Information

The criteria we will use to determine the period of time that we will retain the categories personal information described above depends on our relationship with you and on the following criteria:

- **Laws and regulations**. We are a regulated financial institution that is subject to laws and regulations governing our retention of personal information of our members, applicants for credit union membership, loans and other financial products and services. We are also an employer and,

thus, we are subject to labor laws governing how long we must retain information about applicants for employment and current and former employees. Therefore, applicable laws and regulations will govern how long we retain your personal information.

- **Contracts**. We must also retain information for as long as necessary to comply with our contractual duty to you as well as our contractual obligations with our service providers, contractors and other third-parties.

- **Assert and defend against legal actions**. We may retain your personal information for such period as we may need to assert and defend against potential legal actions.

Contact Information

If you have any questions or comments about this notice, please do not hesitate to contact us at: (800) 649-0193, HR@1stunitedcu.org, and/or5901 Gibraltar Dr. Pleasanton, CA 94588. Please visit our CCPA Privacy Policy on our website www.1stunitedcu.org for more information about the ways in which we collect and use your personal information and your choices and rights regarding such use under California law.