

Collection and Use of Biometric Information

General Statement of Purpose

Corporate America Family Credit Union, CAFCU, maintains policies and procedures that require collection of certain “biometric identifiers” from its employees. CAFCU recognizes the sensitive nature of such biometric identifiers, and the biometric information that is based on an employee’s biometric identifiers and therefore is committed to protecting such information with the same care and diligence that it uses to protect other confidential and sensitive information maintained by CAFCU. In an effort to further this commitment, this policy: (i) establishes guidance for the collection, retention, and treatment of biometric information obtained or received by CAFCU; and (ii) establishes procedures and guidelines for destroying biometric information.

This policy shall be provided to employees and made generally available through CAFCU’s employee handbook. This policy will also be made publicly available on CAFCU’s Intranet.

Biometric Information Collected and Utilized by CAFCU

According to applicable law, biometric identifiers may include retina or iris scans, fingerprints, voiceprints, or scans of hand or facial geometry. Biometric identifiers do not include any of the following items: writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers also do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act or information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

CAFCU collects employee finger prints, and utilizes them in connection with its computer room access procedures. Specifically, employees are required to scan their fingerprint when they access a server room to confirm it is in fact that employee gaining access.

Collection of Biometric Information

In addition to the general notice provided in this policy, each employee is provided with specific written notice when CAFCU wishes to obtain biometric identifiers from him or her. Such notice includes a description of the purpose for which CAFCU intends to use the information and how

long the information will be stored and used. Upon receipt of such notice, the employee will be required to sign, as a condition of employment, a written release consenting to CAFCU's collection of the employee's biometric information.

Retention of Biometric Information

Biometric identifiers collected under this policy, and any biometric information that is based on an employee's biometric identifiers will be retained until such time as the employee's employment with CAFCU is terminated, and will be destroyed no later than 30 days after the date of separation from employment. All biometric identifiers and biometric information derived from identifiers shall be maintained in secured files to which only the SVP of Operations and VP of Human Resources shall have full access. They never have access to the actual identifiers. The security measures used to protect biometric identifiers and biometric information will be at least as rigorous as those measures used to protect CAFCU's other confidential and sensitive information. The information is destroyed/deleted from the security PC by the SVP of Operations or the VP of Human Resources within 5 business days of an employee's termination date

Nothing in this policy shall be construed to prohibit CAFCU from maintaining certain records derived from the use of the employee's biometric identifiers or biometric information (for instance, the employee's finger prints for server access) for a longer period of time in CAFCU's discretion and/or as required by law.

CAFCU will not sell, lease, trade, or otherwise disseminate or disclose an employee's biometric identifiers or biometric information unless and until (1) the employee provides written consent to the disclosure; (2) CAFCU is compelled to disclose the biometric information pursuant to a valid warrant or subpoena; or (3) CAFCU is required to disclose the information under a federal or state law or municipal ordinance.