A bill to be entitled

An act relating to biometric information privacy; creating s. 501.172, F.S.; providing a short title; providing definitions; establishing requirements and restrictions on private entities as to the use, collection, and maintenance of biometric identifiers and biometric information; creating a private cause of action for relief for violations of the act; providing for construction; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 501.172, Florida Statutes, is created to read:

501.172 Biometric information privacy.—

(1) SHORT TITLE.—This section may be cited as the "Florida Biometric Information Privacy Act."

(2) DEFINITIONS.—As used in this section, the term:

(a) "Biometric identifier" means a retina or iris scan, fingerprint, voice print, or scan of hand or face geometry. The term does not include any of the following:

1. 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.

2. Donated organs, tissues, parts, or blood or serum that is stored on behalf of recipients, or potential recipients, of living or cadaveric transplants and that are obtained by or stored by a federally designated organ procurement organization.

3. 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.

4. 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.

(b) "Biometric information" means any information, regardless of the manner in which it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. The term does not include information derived from items or procedures excluded from the definition of biometric identifiers as specified in paragraph (a).

(c) "Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property which includes, but is not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an

account or property, an account number, a PIN number, a pass code, a driver license number, a Florida identification card number, or a social security number.

(d) "Private entity" means any individual, partnership, corporation, limited liability company, association, or other group. The term does not include a state or local governmental agency or any state court, a clerk of the court, or a judge or justice thereof.

(e) "Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

(3) REQUIREMENTS OF PRIVATE ENTITIES.—

(a) A private entity that is in possession of biometric identifiers or biometric information shall develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information upon satisfaction of the initial purpose for collecting or obtaining such identifiers or information or within 3 years after the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) A private entity may not collect, capture, purchase,



CODING: Words stricken are deletions; words underlined are additions.

receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information unless the private entity:

1. Informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

2. Informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

3. Receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) A private entity in possession of a biometric identifier or biometric information may not sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) A private entity in possession of a biometric identifier or biometric information may not disclose or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

1. The subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure;

2. The disclosure completes a financial transaction

requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

3. The disclosure is required by state or federal law or local ordinance; or

4. The disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall store, transmit, and protect from disclosure all biometric identifiers and biometric information:

1. Using the reasonable standard of care within the private entity's industry; and

2. In a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

(4) CAUSE OF ACTION.—Any person aggrieved by a violation of this section has a cause of action in circuit court against an offending party. A prevailing party may recover for each violation:

(a) Liquidated damages of $1,000 or actual damages, whichever amount is greater, against a private entity that negligently violates any provision in subsection (3).

(b) Liquidated damages of $5,000 or actual damages, whichever amount is greater, against a private entity that

intentionally or recklessly violates any provision in subsection (3).

(c) Reasonable attorney fees.

(d) Other relief, including an injunction, as the court deems appropriate.

(5) CONSTRUCTION.—This section may not be construed to:

(a) Impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person;

(b) Conflict with the federal Health Insurance Portability and Accountability Act of 1996 and any regulations promulgated pursuant to that act;

(c) Apply to a contractor, subcontractor, or agent of a state agency or local unit of government when working for that state agency or local unit of government; or

(d) Apply to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and any regulations promulgated pursuant to that act.

Section 2. This act shall take effect October 1, 2019.