AN ACT
RELATING TO HEALTH AND SAFETY -- BIOMETRIC INFORMATION PRIVACY PROTECTION ACT

Introduced By: Representatives Edwards, Canario, Shanley, and Barros

Date Introduced: April 03, 2019

Referred To: House Corporations

It is enacted by the General Assembly as follows:

SECTION 1. Title 23 of the General Laws entitled "HEALTH AND SAFETY" is hereby amended by adding thereto the following chapter:

CHAPTER 95
BIOMETRIC INFORMATION PRIVACY PROTECTION ACT

This chapter shall be known and may be cited as the "Biometric Information Privacy Protection Act."

23-95-2. Legislative findings.
It is hereby found and declared as follows:

(1) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings;

(2) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed.

Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions;

(3) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information;
Despite limited state law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions;

The full ramifications of biometric technology are not fully known; and

The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.


As used in this chapter, the following words and phrases have the following meanings:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include 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 do not include donated organs, tissues, parts, 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 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.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are 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's license number, or a social security number.

"Collect" means the capture, purchase, or acquisition of a person's biometric identifier.

"Private entity" means any individual, partnership, corporation, limited liability
company, association, or other group, however organized. A private entity does not include a state or local government agency.

(6) "Retain" means to collect and store a biometric identifier in whatever form for future use as an identifier of an individual.

(7) "Security purpose" means the purpose of preventing shoplifting, theft or fraud.

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

23-95-4. Retention, collection and destruction.

(a) A private entity in possession of biometric identifiers or biometric information shall develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three (3) years of 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) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(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) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, 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 or redisclosure;

(2) The disclosure or redisclosure 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 or redisclosure is required by state or federal law or municipal 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:

(1) Store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) Store, transmit, and protect from disclosure all biometric identifiers and biometric information 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.

23-95-5. Exceptions.

The provisions of § 23-95-4 shall not apply to:

(1) Law enforcement and correctional custody, including, but not limited to, the identification of perpetrators, prisoners, missing persons, trafficking victims, or human remains;

(2) Facial images used to create driver's licenses or other state identification cards;

(3) Purposes authorized and conducted pursuant to state or federal law;

(4) The retention of voices for quality assurance purposes;

(5) Third-party data storage providers or data transmitters, including Internet service providers or mobile carriers, who provide for the storage or transmittal of data only;

(6) Instances where a person's biometric identifier is captured and stored within the person's own mobile device, computer device, or home security device where biometric identifiers are captured and stored locally within the device and the biometric identifiers do not transmit away from the device using the Internet or other network;

(7) Information collected or retained exclusively for scientific research;

(8) Government security-clearance related programs, research and projects; and

(9) Information used solely and exclusively for security purposes.


(a) Nothing in this chapter shall be construed to 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) Nothing in this chapter shall be construed to conflict with the federal Health Insurance Portability and Accountability Act of 1996.
(c) Nothing in this chapter shall be deemed to apply in any manner 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 the rules promulgated thereunder.

(d) Nothing in this chapter shall be construed to 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.


Any person aggrieved by a violation of this chapter shall have a right of action in a state
court or as a supplemental claim in federal district court against an offending party. A prevailing
party may recover for each violation:

(1) Against a private entity that negligently violates a provision of this chapter, liquidated
damages of one thousand dollars ($1,000) or actual damages, whichever is greater;

(2) Against a private entity that intentionally or recklessly violates a provision of this
chapter, liquidated damages of five thousand dollars ($5,000) or actual damages, whichever is
greater; and

(3) Reasonable attorneys' fees and costs.

23-95-8. Enforcement by attorney general.

Whenever the attorney general has reason to believe that a person or private entity has
violated the provisions of this chapter, and that proceeding would be in the public interest, the
attorney general may bring an action in the name of the state or on behalf of persons residing in
the state, against the person or private entity to restrain and enjoin the use of methods, acts or
practices that are in violation of this chapter.


If any part of this chapter shall be deemed invalid, all valid parts that are severable shall
remain in full force and effect.

SECTION 2. This act shall take effect upon passage.

======
LC002323
======
EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO HEALTH AND SAFETY -- BIOMETRIC INFORMATION PRIVACY PROTECTION ACT

***

1 This act would prohibit the collection and retention of biometric identifiers without consent of the person whose information is collected. Exceptions would be law enforcement, government use, research and government security-clearance related projects.

2 This act would take effect upon passage.