# Department of Legislative Services

Maryland General Assembly
2020 Session

## FISCAL AND POLICY NOTE
## Third Reader - Revised

House Bill 307 (Delegate Love, *et al.*)
Economic Matters Finance

**Commercial Law - Consumer Protection - Biometric Identifiers and Biometric Information Privacy**

This bill generally requires each "private entity" in possession of "biometric identifiers" or "biometric information" to develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying the biometric identifiers and information on the earlier of (1) when the initial purpose for collecting or obtaining the biometric identifiers or information has been satisfied or (2) within three years after the individual's last interaction with the private entity. Absent a valid warrant or subpoena, each private entity in possession of biometric identifiers or information must comply with the retention schedule and destruction guidelines. The bill establishes various other standards and requirements related to biometric identifiers and information, including authorizing an aggrieved individual to bring a civil action against a private entity that violates the bill's requirements. **The bill takes effect January 1, 2021.**

## Fiscal Summary

**State Effect:** The bill is not anticipated to materially affect State finances or operations.

**Local Effect:** The bill is not anticipated to materially affect local government finances or operations.

**Small Business Effect:** Potential meaningful.

## Analysis

**Bill Summary:** A "biometric identifier" means the data of an individual generated by automatic measurements of an individual's biological characteristics that can be used to uniquely authenticate the individual's identity.

"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. A "private entity" is any individual, partnership, corporation, limited liability company, association, or other group, however organized; it does not include a business (or an affiliate) subject to and in compliance with the federal Graham-Leach-Bliley Act (a financial institution like a bank).

Each private entity in possession of biometric identifiers or biometric information must store, transmit, and protect the biometric identifiers and information from disclosure (1) using the reasonable standard of care within the private entity's industry and (2) in a manner that is as protective as (or more protective than) the manner that the private entity stores, transmits, and protects other confidential and sensitive information.

A private entity may not collect, capture, purchase, receive through trade, or otherwise obtain an individual's biometric identifiers or information unless the private entity first informs the individual (or the individual's legally authorized representative) in writing (1) that biometric identifiers or information is being collected or stored and (2) of the specific purpose and length of time that biometric identifiers or information is being collected, stored, or used. The private entity must also receive a written release executed by the individual (or the individual's legally authorized representative).

A private entity in possession of biometric identifiers or information is prohibited from selling, leasing, trading, or otherwise profiting from an individual's biometric identifiers or biometric information. In addition, such entities may not disclose, redisclose, or otherwise disseminate an individual's biometric identifiers or information unless:

- the individual (or the individual's legally authorized representative) consents to the disclosure or redisclosure;
- the disclosure or redisclosure is necessary to complete a financial transaction requested by the individual (or the individual's legally authorized representative);
- the disclosure or redisclosure is required by law; or
- the disclosure or redisclosure is required by a valid warrant or subpoena.

A private entity is not required to make publicly available a written policy required by the bill if the policy (1) applies only to the employees of the private entity and (2) is used solely for internal company operations.

*Civil Actions*

An individual who prevails in a civil action under the bill may recover:

- against a private entity that negligently violated a provision of the bill, $1,000 or actual damages, whichever is greater;

- against a private entity that intentionally or recklessly violated a provision of the bill, $5,000 or actual damages, whichever is greater;

- reasonable attorney's fees and costs, including expert witness fees and other litigation expenses; and

- other relief, including an injunction, as the court may determine appropriate.

**Current Law:** The Maryland Personal Information Protection Act (MPIPA) defines "personal information" as, among other things, biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account in combination with an individual's first name or first initial and last name, when the name or data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.

Under MPIPA, when a business is destroying a customer's, employee's, or former employee's records containing personal information, the business must take reasonable steps to protect against unauthorized access to or use of the personal information, taking specified considerations into account.

To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of a Maryland resident must implement and maintain reasonable and appropriate security procedures and practices. A business that uses a nonaffiliated third party as a service provider and discloses personal information about a Maryland resident under a written contract with the third party must require, by contract, that the third party implement and maintain reasonable security procedures and practices that are (1) appropriate to the nature of the disclosed information and (2) reasonably designed to help protect the information from unauthorized access, use, modification, disclosure, or destruction. This provision applies to a written contract that is entered into on or after January 1, 2009.

A business that owns, licenses, or maintains computerized data that includes personal information of a Maryland resident, upon the discovery or notification of a breach of the security of a system, must conduct, in good faith, a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused as a result of the breach. If, after the investigation, the business reasonably believes that the breach has resulted or will result in the misuse of personal information of a Maryland resident, the business must notify the individual of the breach. Generally, the notice must be given as soon as reasonably practicable (but no later than 45 days after the business conducts the required investigation). If the business determines that notification is not required, the business must maintain the records related to the determination for three years.

A business that maintains computerized data that includes personal information that it does not own or license must notify the owner or licensee of the personal information of a breach and share information relevant to the breach as soon as reasonably practicable (but no later than 45 days) after the business discovers or is notified of the breach. Such a third-party business may not charge a fee for providing the information needed for the required notification to the owner or licensee of the data. Moreover, the owner or licensee may not use information relative to the breach for purposes other than (1) providing notification of the breach; (2) protecting or securing personal information; or (3) providing notification to national information security organizations created for information sharing and analysis of security threats, to alert and avert new or expanded breaches.

Required notifications may be delayed (1) if a law enforcement agency determines that it will impede a criminal investigation or jeopardize homeland or national security or (2) to determine the scope of the breach, identify the individuals affected, or restore the system's integrity.

Consumer notification must include a description of categories of information acquired by the unauthorized user, the business' contact information, and contact information for the major consumer reporting agencies and specified government agencies. The notification may be given by mail or telephone; electronic mail or other forms of notice may be used if specified conditions are met. Prior to consumer notification, a business must notify the Office of the Attorney General of the breach after it discovers or is notified of the breach.

In the case of a breach of a security system involving an individual's email account – but no other specified personal information – the business may comply with the required notification in electronic or other form. The notification must direct the individual whose personal information has been breached to promptly (1) change the individual's password and security question or answer, as applicable, or (2) take other appropriate steps to protect the email account, as well as all other online accounts for which the individual uses the same user name or email and password (or security question or answer).

Generally, the required notification may be given to the individual by any method described in § 14-3504 of the Commercial Law Article. However, the required notification may not be given by sending notification by email to the affected account. The notification *may*, however, be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected email account from an Internet protocol address or online location from which the business knows the individual customarily accesses the account.

A waiver of the notification requirements is void and unenforceable. Compliance with the notification requirements does not relieve a business from a duty to comply with any federal legal requirements relating to the protection and privacy of personal information.

**Small Business Effect:** Any small businesses in the State that handle biometric identifiers or information may need to develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information within the time period required by the bill (to the extent that such businesses have not already developed such policies and procedures). The bill also prohibits private entities from selling, leasing, trading, or otherwise profiting from an individual's biometric information or biometric information, which may significantly impact any small businesses that currently engage in such activities.

## Additional Information

**Prior Introductions:** None.

**Designated Cross File:** None.

**Information Source(s):** Judiciary (Administrative Office of the Courts); Department of Legislative Services

**Fiscal Note History:** First Reader - February 25, 2020
rh/ljm Third Reader - March 17, 2020
Revised - Amendment(s) - March 17, 2020

Analysis by: Eric F. Pierce

Direct Inquiries to:
(410) 946-5510
(301) 970-5510