Department of Legislative Services

Maryland General Assembly
2021 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 148 (Delegate Carey)
Economic Matters Finance

Commercial Law - Personal Information Protection Act - Revisions

This bill expands the Maryland Personal Information Protection Act (MPIPA) by (1) covering additional types of personal information; (2) expanding the types of businesses that are required to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized use; (3) shortening the period within which certain businesses must provide required notifications to consumers after a data breach; (4) modifying the standard for using a substitute notification method; and (5) requiring additional information to be provided to the Office of the Attorney General (OAG) after a breach has occurred. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.

Fiscal Summary

State Effect: The bill's imposition of existing penalty provisions does not have a material impact on State finances or operations. OAG, Consumer Protection Division, can handle the bill's requirements with existing resources.

Local Effect: The bill's imposition of existing penalty provisions does not have a material impact on local government finances or operations.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary: The bill expands the definition of "personal information" under MPIPA to include genetic information of an individual, as specified.

Security Procedures

The bill requires a business that maintains (in addition to a business that owns or licenses) personal information of a Maryland resident to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information maintained and the nature and size of the business and its operations.

Security Breaches

For a business that owns, licenses, or maintains personal data, unless the business reasonably determines that a breach *does not create a likelihood* that personal information has been (or will be) misused, the business must notify the individual of the breach. Generally, the required notification must be given as soon as reasonably practicable and must be provided within 45 days after the business discovers (or is notified) of the breach.

For a business that maintains personal data, generally, the business must notify the owner or licensee of the breach as soon as practicable; however, the bill requires the notification to be provided within 10 days (rather than 45 days) after the business discovers (or is notified) of the breach.

If a required notification is delayed because a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security, notification must be given as soon as reasonably practicable, but no later than 7 days (rather than 30 days) after the law enforcement agency makes the required determination.

Standard for and Method of Substitute Notice for Notification of Affected Individuals

The bill modifies both the standard for and a specific method associating with using the three-pronged substitute notice method in the event a business discovers (or is notified) a data breach has occurred. Substitute notice may *only* be used if the business does not have sufficient contact information to give notice through one of the regular (and more direct) methods. Substitute notice is no longer allowed for a demonstration that the regular methods of notice would be costly (more than $100,000) or the number of affected individuals exceeds a certain threshold (175,000). When substitute notice has to be used, it must include notification to major print or broadcast media in geographic areas where the individuals affected by the breach likely reside (rather than to statewide media).

Contents of Notice to the Office of the Attorney General

For data breaches involving a business that owns, licenses, or maintains personal information, the bill expands the information that must be included in a notice provided to OAG. At a minimum, the notice must include:

- the number of affected Maryland residents;
- a description of the breach, including when and how it occurred;
- any steps the business has taken (or plans to take) relating to the breach of the security of a system; and
- the form of notice that will be sent to affected individuals and a sample notice.

Current Law:

Maryland Personal Information Protection Act

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 owner or licensee of the data must notify the individual of the breach. Generally, the notice to the individual 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 OAG 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.

Violation of MPIPA is an unfair, abusive, or deceptive trade practice under MCPA, subject to MCPA's civil and criminal penalty provisions.

Maryland Consumer Protection Act

An unfair, abusive, or deceptive trade practice under MCPA includes, among other acts, any false, falsely disparaging, or misleading oral or written statement, visual description, or other representation of any kind that has the capacity, tendency, or effect of deceiving or misleading consumers. The prohibition against engaging in any unfair, abusive, or deceptive trade practice encompasses the offer for or actual sale, lease, rental, loan, or bailment of any consumer goods, consumer realty, or consumer services; the extension of consumer credit; the collection of consumer debt; or the offer for or actual purchase of consumer goods or consumer realty from a consumer by a merchant whose business includes paying off consumer debt in connection with the purchase of any consumer goods or consumer realty from a consumer.

The Consumer Protection Division is responsible for enforcing MCPA and investigating the complaints of aggrieved consumers. The division may attempt to conciliate the matter, issue a cease and desist order, or file a civil action in court. A merchant who violates MCPA is subject to a fine of up to $10,000 for each violation and up to $25,000 for each repetition of the same violation. In addition to any civil penalties that may be imposed, any person who violates MCPA is guilty of a misdemeanor and, on conviction, is subject to a fine of up to $1,000 and/or imprisonment for up to one year.

Small Business Effect: The bill's further expansion of and modifications to MPIPA may result in additional costs for small businesses that own, license, or maintain the personal information of Maryland residents. Specifically, should notification to affected individuals be required (particularly within the shortened timeframe under the bill), businesses cannot use the substitute notice methods merely because the number of affected individuals or the cost to provide regular (and more direct) notice exceeds certain thresholds.

Otherwise, the effect of the bill on small businesses is generally limited to those that *maintain* data and the need to come into compliance with MPIPA's other data security requirements. Under Chapters 294 and 295 of 2019, MPIPA was expanded to require any business that maintains computerized data that includes the personal information of a Maryland resident that is subject to a breach to conduct a reasonable and prompt investigation when the business discovers (or is notified) that it incurred a security breach. If a misuse of personal information has occurred (or is reasonably likely to occur) the

business must notify the affected individual of the breach. As a result of these existing requirements, many small businesses that maintain the personal information of Maryland residents may have *voluntarily* chosen to come into compliance with other data security requirements. However, Chapters 294 and 295 do not *require* such businesses to do so. It is unclear how many small businesses in the State that maintain personal information may already be in compliance with MPIPA's data security requirements. For those that have already come into compliance, the bill likely has minimal or no effect due to this broadening of scope. Other businesses maintaining personal information may need to improve their security procedures and practices, resulting in additional compliance costs.

Additional Information

Prior Introductions: SB 201 of 2020, a similar bill, received a hearing in the Senate Finance Committee, but no further action was taken. Its cross file, HB 237, received a hearing in the House Economic Matters Committee, but no further action was taken.

Designated Cross File: SB 112 (Senator Lee) - Finance.

Information Source(s): Office of the Attorney General; Department of Legislative Services

Fiscal Note History: First Reader - January 24, 2021
rh/ljm Third Reader - April 2, 2021
Revised - Amendment(s) - April 2, 2021
Revised - Clarification - April 2, 2021

Analysis by: Eric F. Pierce

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