HB 1154

Department of Legislative Services

Maryland General Assembly
2019 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

House Bill 1154 (Delegate Howard, *et al.*)
Economic Matters Finance

Maryland Personal Information Protection Act - Security Breach Notification Requirements - Modifications

This bill expands the types of businesses that are required to provide notification to consumers of data breaches under the Maryland Personal Information Protection Act (MPIPA). Under the bill, any business that maintains (in addition to any business that owns or licenses) computerized data that includes the personal information of a Maryland resident that is subject to a breach must 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. 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. The Office of the Attorney General (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 prohibits a third-party business from charging a fee for providing the information needed for the required notification to the owner or licensee of the data. 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.

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 or licenses 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 not 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 not later than 45 days) after the business discovers or is notified of the breach.

The notification 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.

MPIPA is exclusive and preempts any provision of local law.

If a business is required to give notice of a breach to 1,000 or more individuals, the business must also notify, without unreasonable delay, specified consumer reporting agencies of the

timing, distribution, and content of the notices. However, the business is not required to include the names or other personal information about the notice recipients.

Businesses that comply with the requirements for notification procedures, the protection or security of personal information, or the destruction of personal information under the rules, regulations, procedures, or guidelines established by their primary or functional federal or State regulators are deemed in compliance with MPIPA. Likewise, businesses or their affiliates that comply with specified federal acts and regulations governing the protection of information are also deemed in compliance with MPIPA.

Unfair, Abusive, or Deceptive Trade Practices

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 which 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.

Background: In February 2019, the Consumer Sentinel Network, a consortium of national and international law enforcement and private security entities, released the *Consumer Sentinel Network Data Book* for calendar 2018. In calendar 2018, the Federal Trade Commission (FTC) received 444,602 identity theft complaints nationwide compared to 371,061 in calendar 2017 and 399,225 in calendar 2016.

In Maryland, residents reported 8,747 instances of identity theft in 2018, or 145 complaints per 100,000 population, ranking Maryland seventh in the nation for identity theft. In 2017, Maryland ranked fourth in the nation for identity theft. The most common type of identity theft in Maryland was credit card fraud, which comprised 37% of all complaints.

According to OAG, there were 993 security breach incidents in 2018 that required notifications to be sent to Maryland consumers, compared to 1,084 in 2017 and 792 in 2016.

Exhibit 1 shows the number of security breaches reported to OAG as well as the number of identity complaints received by FTC.

Exhibit 1
Security Breaches and Identity Theft Complaints in Maryland
2016-2018

	2016	2017	2018	Average (2016-18)
Security Breaches Reports	792	1,084	993	**956**
Identity Theft Complaint Reports	8,251	7,788	8,747	**8,262**

Source: Office of the Attorney General; Federal Trade Commission

The federal Gramm-Leach-Bliley Act (GLB Act) requires financial institutions to protect the security and confidentiality of their customers' nonpublic personal information. MPIPA specifically references the GLB Act and states that any business subject to and in compliance with the GLB Act is considered to be in compliance with MPIPA.

Small Business Effect: Under the bill, any businesses that store information on behalf of other businesses are potentially subject to the direct consumer notification requirements of MPIPA. Thus, such businesses may incur additional costs to notify consumers.

Additional Information

Prior Introductions: A similar bill as amended, HB 1584 of 2018, passed the House and was referred to the Senate Finance Committee, but no further action was taken. HB 965 of 2017, a similar bill, passed the House as amended and received a hearing in the Senate Finance Committee, but no further action was taken.

Cross File: SB 693 (Senator Kramer, *et al.*) - Finance.

Information Source(s): Office of the Attorney General (Consumer Protection Division); Judiciary (Administrative Office of the Courts); Department of Information Technology;

Consumer Sentinel Network; Federal Trade Commission; Department of Legislative Services

Fiscal Note History: First Reader - March 5, 2019
mag/kdm Third Reader - March 25, 2019
Revised - Amendment(s) - March 25, 2019

Analysis by: Eric F. Pierce

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