SB 552

Department of Legislative Services

Maryland General Assembly
2017 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 552 (Senator Hershey)
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* (rather than 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 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. If the Consumer Protection Division of the Office of the Attorney General (OAG) receives fewer than 50 complaints per year stemming from the bill, the additional workload can be handled 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 also alters what a business that owns or licenses computerized data may do after the business receives a notice from a third-party business that maintains the owner's or licensee's data that a security breach of the data has occurred, which has resulted in, or is likely to result in, the misuse of personal information. The business owner or licensee of the computerized data that was subject to a breach may elect to notify affected individuals of the security breach on behalf of the business that is responsible for maintenance and security of the data and incurred the breach. The business owner or licensee of the computerized data is not required to make this election, nor can the third-party business responsible for data maintenance compel the business owner or licensee to undertake such notifications.

The bill also expands the duty to comply with notification procedures to those Maryland businesses that are subject to, and in compliance with, specified federal laws and regulations. Accordingly, those businesses that are compliant with those laws are also considered to be in compliance with the security procedures established in MPIPA. However, those Maryland businesses must still comply with the notification procedures established in MPIPA in the event of a security breach of computerized data.

Current Law:

Maryland Personal Information Protection Act

When a business is destroying a customer's records containing the customer's 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 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 if it is likely that it has resulted or will result in the misuse of personal information of a Maryland resident. Generally, the notice must be given as soon as reasonably practicable 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.

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 or Deceptive Trade Practices

An unfair 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 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 $1,000 for the first violation and up to $5,000 for each subsequent 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: 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 2015. In calendar 2015, the Federal Trade Commission received 490,220 identity theft complaints. In calendar 2014, the number of identity theft complaints was 332,647, compared to 290,102 in calendar 2013. In Maryland, residents reported 11,006 instances of identity theft in 2014, or 183.2 complaints per 100,000 population, ranking Maryland fourth in the nation for identity theft. This was a significant increase compared to 2014, when residents reported 5,734 instances of identity theft (95.9 complaints per 100,000 population). In 2014, Maryland ranked tenth in the nation for identity theft. The most common type of identity theft in Maryland was government documents or benefits fraud, which comprised 57% of all complaints. The second most prevalent type of identity fraud involved credit card fraud and represented 14% of all complaints.

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. (Under the

bill, businesses that comply with the GLB Act are still considered to be in compliance with the required security procedures of MPIPA; however, they may no longer be considered in compliance with the *entirety* of MPIPA.)

According to OAG, there were 497 security breach notices sent in 2016 to Maryland consumers as required by MPIPA, compared to 482 in 2015 and 333 in 2014.

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 as a result of the bill. On the other hand, businesses that own or license personal data, but rely on third parties to store personal information of consumers, may no longer be subject to consumer notification requirements, to the extent that such businesses elect not to notify consumers whose data has been breached on behalf of the third-party business that actually incurred the breach. For those businesses, notification costs could decline.

Additional Information

Prior Introductions: None.

Cross File: HB 965 (Delegate S. Howard, *et al.*) - Economic Matters.

Information Source(s): Department of Information Technology; Office of the Attorney General; Judiciary (Administrative Office of the Courts); Consumer Sentinel Network; Federal Trade Commission; Department of Legislative Services

Fiscal Note History: First Reader - February 22, 2017
mm/kdm

Analysis by: Eric Pierce

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