SB 525

Department of Legislative Services

Maryland General Assembly
2017 Session

FISCAL AND POLICY NOTE
Third Reader - Revised

Senate Bill 525 (Senator Lee, *et al.*)
Finance Rules and Executive Nominations

Maryland Personal Information Protection Act - Revisions

This bill expands the Maryland Personal Information Protection Act (MPIPA) to impose additional duties on a business to protect an individual's personal information. In addition, the bill alters notification procedures when a business experiences a security breach. Finally, the bill establishes a specific notification process for breaches involving email account information.

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.

The bill takes effect January 1, 2018.

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:

Definitions

The bill alters the definition of "encrypted" to mean the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.

The bill defines "health information" as any information created by an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) regarding an individual's medical history, medical condition, or medical treatment or diagnosis.

In addition to data elements under current law, the bill alters the definition of "personal information" to encompass the following data elements: (1) a passport number or other identification number issued by the federal government; (2) a State identification card number; (3) health information, including information about an individual's mental health; (4) a health insurance policy or certificate number or health insurance subscriber identification number in combination with a unique identifier issued by an insurer (or any employer that is self-insured) that permits access to an individual's health information; and (5) specified biometric data of an individual that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account.

The definition of "personal information" is also expanded to include a user name or email address in combination with a password or security question and answer that permits access to an individual's email account.

Protection Against Unauthorized Access or Use

When a business is destroying records that contain personal information, the entity must also take reasonable steps to protect the information of employees or former employees, in addition to customers, as specified.

Security Breaches

The bill establishes that, if a business determines that a breach creates a likelihood that personal information has been (or will be) misused, the business must notify an affected individual as soon as practicable, but not later than 45 days after the business concludes its investigation.

The bill requires a business that maintains computerized data that includes personal information of a Maryland resident that it does not own or license to notify the owner or licensee of the personal information upon discovery or notification of the breach. The bill requires the business to provide this notice as soon as reasonably practicable but not later than 45 days after the business discovers or is notified of the breach.

Procedures for Breaches of Email Accounts

The bill also establishes a specific notification process for breaches involving email account information. In the case of a breach of a security system involving an individual's email account (as defined by the bill) – 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 MPIPA. 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.

Compliance with the Maryland Personal Information Protection Act

The bill establishes that a business that is subject to and in compliance with HIPAA is deemed to be in compliance with MPIPA. Likewise, an affiliate that is compliance with HIPAA is deemed to be in compliance with MPIPA.

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: In March 2017, 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 2016. In calendar 2016, the Federal Trade Commission (FTC) received 399,225 identity theft complaints nationwide compared to 490,226 in calendar 2015 and 332,647 in calendar 2014.

In Maryland, residents reported 8,251 instances of identity theft in 2016, or 137.1 complaints per 100,000 population, ranking Maryland seventh in the nation for identity theft. In 2015, Maryland ranked fourth in the nation for identity theft. The most common type of identity theft in Maryland was employment- or tax-related fraud, which comprised 39% of all complaints. The second most prevalent type of identity fraud involved credit card fraud and represented 31% of all complaints.

According to OAG, there were 790 security breach incidents in 2016 that required notifications to be sent to Maryland consumers, compared to 482 in 2015 and 333 in 2014.

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
2014-2016[1]

	2014	2015	2016	Average (2014-16)
Security Breaches Reports	333	482	790	**535**
Identity Theft Complaint Reports	5,734	11,006	8,251	**8,330**

[1]Security breaches are reported to the Office of the Attorney General (OAG) and are totaled by fiscal year; identity theft complaints are reported to the Federal Trade Commission (FTC) and are totaled by calendar year. Numbers reflect those reported to OAG or FTC as of March 11, 2017.

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: The bill may create meaningful expenditures for small businesses that experience a security breach and are required to protect additional types of information as specified in the bill. The bill's time limits regarding how soon businesses must notify individuals of a breach may also result in additional expenditures for small businesses.

Additional Information

Prior Introductions: SB 548 of 2015, a similar bill, received a hearing in the Senate Finance Committee, but no further action was taken.

Cross File: HB 974 (Delegates Carey and Lisanti) - Economic Matters.

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

Fiscal Note History: First Reader - February 22, 2017
md/kdm Third Reader - April 8, 2017
Revised - Amendment(s) - April 8, 2017
Revised - Updated Information - April 8, 2017

Analysis by: Eric Pierce

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