SB 548

Department of Legislative Services

Maryland General Assembly
2015 Session

FISCAL AND POLICY NOTE

Senate Bill 548 (Senator Lee)
Finance

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 private information, including the implementation of reasonable security procedures and practices. The bill also alters the standard to be evaluated when determining whether a business must take specified actions to protect an individual's private 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.

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 alters the definition of "encrypted" to mean the protection of data in electronic or optical form, in storage or in transit, using an encryption technology that (1) has been adopted by an established standards-setting body of the federal government,

including the Federal Information Processing Standards issued by the National Institute of Standards and Technology and (2) renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data.

The bill alters the definition of "personal information" to mean any information relating to an individual, including name, number, personal mark, unique biometric or genetic print, image, or data, or any other identifier, that can be used to identify the individual.

The bill defines "private information" as personal information in combination with any one or more of the following data elements, whether or not any of the elements are encrypted: (1) a Social Security number; (2) a driver's license number or State identification card number; (3) a passport number or other identification number issued by the United States; or (4) an account number or credit or debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's financial account.

Additionally, the bill defines "reasonable security procedures and practices" as data security procedures and practices developed in good faith and set forth in a written information security policy that clearly demonstrates that the procedures and practices:

- coordinate an information security program;
- require a risk assessment to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and to assess the sufficiency of any safeguards in place to control the risks;
- once a risk assessment is completed, include design safeguards to control the identified risks and to regularly monitor the controls' effectiveness;
- ensure, in any contract with a service provider, that the service provider is capable of providing appropriate safeguards for customers' personal information and private information; and
- evaluate and adjust the information security program based on specified criteria.

The requirement to implement and maintain reasonable security procedures and practices for a business that uses a nonaffiliated third party as a service provider under a written contract applies prospectively and does not apply to a written contract that is entered into before January 1, 2016.

The bill requires a business that owns or licenses computerized data that includes private information of a Maryland resident, upon the discovery or notification of a breach of the security of a system, to conduct, in good faith, a reasonable and prompt investigation to determine whether the unauthorized acquisition of private information of the individual has been created or is reasonably likely to create a material risk of identity fraud, as defined

by the bill. If the business makes an affirmative determination, the bill requires the business to notify the individual within 45 days.

The bill requires a business that maintains computerized data that includes private information that it does not own or license to notify the owner or licensee of the private information of a breach and share information relevant to the breach if it is likely that the unauthorized acquisition of the individual's private information has created or is reasonably likely to create a material risk of identity fraud. The bill requires the business to provide this notice within 45 days.

If a business is required to give notice of a breach to 1,000 or more individuals, the bill requires the business to also notify, within 45 days, specified consumer reporting agencies of the timing, distribution, and content of the notices.

Current Law: 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.

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 bill's provisions contain proposals of the Maryland Commission on Cybersecurity Innovation and Excellence. The commission was created by Chapters 250 and 251 of 2011 and was charged with producing a comprehensive overview of current State cybersecurity laws and policies and developing recommendations for a coordinated, rapid response to cyber attacks on government networks and computer systems. The commission terminated on December 31, 2014.

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 2014. In calendar 2014, the Federal Trade Commission (FTC) received 332,646 identity theft complaints. In calendar 2013, the number of identity theft complaints was 290,099. In Maryland, residents reported 5,734 instances of identity theft in 2014, or 95.9 complaints per 100,000 population, ranking Maryland tenth in the nation for identity theft. The most common type of identity theft in Maryland was government documents or benefits fraud, which comprised 35% of all complaints. The second most prevalent type of identity fraud involved credit card fraud and represented 18% 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 deemed to be in compliance with MPIPA. Pursuant to the GLB Act, FTC enumerated five elements of reasonable security procedures and practices. These five elements are substantially similar to the bill's definition of reasonable security procedures and practices.

On its website, OAG provides charts detailing security breach notices it has received per calendar year since 2008; in 2014, OAG received 314 security breach notices.

Small Business Effect: The bill may create meaningful expenditures for small businesses that experience a security breach and are required to institute reasonable security procedures and practices. Currently, statute is unclear as to what constitutes reasonable security procedures and practices. However, the bill establishes five tasks that a business, including a small business, must undertake to protect personal and private information. To the extent that such a business does not already implement similar procedures, the enhanced security measures may prove costly.

Additional Information

Prior Introductions: HB 960 of 2013 received an unfavorable report from the House Economic Matters Committee. Its cross file, SB 859, was withdrawn after receiving a hearing in the Senate Education, Health, and Environmental Affairs Committee.

Cross File: None.

Information Source(s): Office of the Attorney General (Consumer Protection Division), Judiciary (Administrative Office of the Courts), Consumer Sentinel Network, Department of Legislative Services

Fiscal Note History: First Reader - March 16, 2015
mar/kdm

Analysis by: Sasika Subramaniam

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