Department of Legislative Services
Maryland General Assembly
2007 Session

FISCAL AND POLICY NOTE
Revised

Senate Bill 194 (Senator Kelley, *et al.*)
Finance Economic Matters

Consumer Protection - Personal Information Protection Act

This bill imposes duties on a "business" to protect an individual's "personal information" and to provide notice of a security breach relating to an individual's personal information. Violation of the bill is an unfair or deceptive trade practice under the Maryland Consumer Protection Act.

The bill takes effect January 1, 2008.

Fiscal Summary

State Effect: Assuming that the Consumer Protection Division receives fewer than 50 complaints per year stemming from this bill, any additional workload could be handled with existing resources.

Local Effect: None.

Small Business Effect: Minimal.

Analysis

Bill Summary: 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 include personal information of a Maryland resident, when it discovers or is notified 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 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 these records for three years.

A business that maintains computerized data that include 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, 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 the Office of the Attorney General of the breach after it discovers or is notified of the breach.

A waiver of the bill's 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.

The bill's provisions are exclusive and preempt any provision of local law.

If a business is required to give notice of a breach under the bill 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 the bill. Likewise, businesses or their affiliates that comply with specified federal acts and regulations governing the protection of information are also deemed in compliance with the bill.

Current Law: A business's practices regarding records that contain personal information is not specifically regulated.

The Consumer Protection Division within the Office of the Attorney General is responsible for pursuing unfair and deceptive trade practice claims under the Maryland Consumer Protection Act. Upon receiving a complaint, the division must determine whether there are "reasonable grounds" to believe that a violation of the Act has occurred. Generally, if the division does find reasonable grounds that a violation has occurred, the division must seek to conciliate the complaint. The division may also issue cease and desist orders, or seek action in court, including an injunction or civil damages, to enforce the Act. Violators of the Act are subject to: (1) civil penalties of $1,000 for the first violation and $5,000 for subsequent violations; and (2) criminal sanction as a misdemeanor, with a fine of up to $1,000 and/or up to one year's imprisonment.

Background: Under the guidelines adopted jointly by federal banking regulators "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that the misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible."

In 2006, the Federal Trade Commission announced that ChoicePoint, Inc. would pay a $10 million civil penalty and $5 million in consumer redress for violating the federal Fair Credit Reporting Act for failing to have adequate protections for wrongfully releasing consumer information. The settlement requires ChoicePoint to implement new procedures: (1) to ensure that it provides consumer reports only to legitimate businesses for lawful purposes; (2) to establish and maintain a comprehensive information security program; and (3) to obtain audits by an independent third-party security professional every other year until 2026.

The TJX Companies, Inc., parent company to TJ Maxx and Marshalls, recently announced a security breach in which many customer credit card numbers were stolen and at least some stolen card numbers were fraudulently used.

At least one bill (S. 239) has been introduced to date in the 110th Congress to regulate notification after the breach of a database containing personal information. S. 239 would require notification and would preempt state notification provisions; it is a reintroduction of a bill from the 109th Congress.

Additional Information

Prior Introductions: An identical bill, SB 134 of 2006 as amended, passed the Senate. It received a hearing in the House Economic Matters Committee, where no further action was taken. A similar bill, HB 1349 of 2006, received a hearing in the Economic Matters Committee, but no further action was taken.

Cross File: HB 208 (Delegate Howard, *et al.*) – Economic Matters.

Information Source(s): Office of the Attorney General (Consumer Protection Division), Federal Trade Commission, Department of Legislative Services

Fiscal Note History: First Reader - February 13, 2007
mll/jr Revised - Senate Third Reader - March 21, 2007
Revised - Enrolled Bill - May 7, 2007

Analysis by: Suzanne O. Potts

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