SB 904

Department of Legislative Services
Maryland General Assembly
2007 Session

FISCAL AND POLICY NOTE

Senate Bill 904 (Senator Dyson)
Finance

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.

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 all reasonable steps to destroy or arrange for the destruction of the records in a manner that makes the information unreadable or undecipherable through any means.

A business that compiles, maintains, or makes available personal information of a Maryland resident must implement and maintain reasonable and appropriate security

procedures and practices to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. A business that discloses personal information under a contract with a nonaffiliated third party must require by contract that the third party comply with these requirements.

A business that compiles, maintains, or makes available records that include a Maryland resident's personal information must notify that individual of a breach of the security of a system if, as a result of the breach, the individual's personal information: (1) has been acquired by an unauthorized person; or (2) is reasonably believed to have been acquired by an unauthorized person. Generally, the notice must be given as soon as practicable after the business discovers or is notified about the breach.

The notification may be delayed: (1) if a law enforcement agency determines that it will impede a criminal investigation; or (2) to determine the scope of the breach and restore the system's integrity.

The notification may be given by written, electronic, telephonic, or substitute notice if specified conditions are met. The notice must include: (1) to the extent possible, a description of the categories of information, including which elements of personal information, that were, or are reasonably believed to have been, acquired; (2) contact information for the business making the notification; (3) specified contact information for the major consumer reporting agencies; and (4) specified contact and other information relating to the Federal Trade Commission and the Office of the Attorney General.

A business must notify the Office of the Attorney General of the breach within 24 hours after it becomes aware 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 other legal requirements relating to the protection and privacy of personal information.

Compliance with a federal or State law is deemed compliance with the bill regarding the subject matter of that law if the law provides: (1) at least the same protections to personal information as the bill; and (2) disclosure requirements that are at least as thorough as the bill's.

In addition to the penalties under the Consumer Protection Act, an individual who is affected by a violation may bring a civil action against a violator to recover reasonable attorney's fees and the greater of $500 per violation or actual damages.

Current Law: A business's practices regarding records that contain personal information are 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 stole 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: Nearly identical bills, SB 486 and HB 630, were introduced during the 2006 session. SB 486 was heard in the Senate Finance Committee and HB 630 was heard in the House Economic Matters Committee. No further action was taken on either bill. Similar bills were introduced during the 2006 and 2005 sessions. SB 134 of 2006 was amended and passed the Senate; it was heard in Economic Matters, but no further action was taken. HB 873 and HB 1179 of 2006 were heard in Economic Matters, but no further action was taken on either bill. SB 1002 of 2005 was referred to the Senate Rules Committee, and HB 1588 of 2005 was referred to Economic Matters. Both bills were withdrawn before being heard.

Cross File: HB 123 (Delegate Lee, *et al.*) – Economic Matters.

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

Fiscal Note History: First Reader - March 2, 2007
ncs/jr

Analysis by: T. Ryan Wilson

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