

Department of Legislative Services
Maryland General Assembly
2007 Session

FISCAL AND POLICY NOTE

House Bill 90
Economic Matters

(Delegate Shewell, *et al.*)

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 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 owns or licenses 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. This provision applies to a written contract entered into on or after January 1, 2009.

A business that owns or licenses computerized data 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 required to notify 1,000 or more individuals must also notify each consumer reporting agency that compiles and maintains files on consumers nationwide under specified circumstances. A business must notify the Office of the Attorney General and the Maryland Department of Homeland Security of the breach within 72 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.

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.

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."

Background: The Federal Trade Commission recently 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 of TJ Maxx and Marshalls, recently announced a security breach in which many customer credit card numbers were stolen and at least some credit 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: Similar bills were introduced during the 2006 session. HB 1349 received a hearing in the House Economic Matters Committee, but no further action was taken. As amended, SB 134 passed the Senate and received a hearing in Economic Matters, where no further action was taken.

Cross File: None.

Information Source(s): State Department of Assessments and Taxation; Department of Labor, Licensing, and Regulation; Office of the Attorney General (Consumer Protection Division); Department of Legislative Services

Fiscal Note History: First Reader - February 12, 2007
ncs/jr

Analysis by: T. Ryan Wilson

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