SB 514

Department of Legislative Services
Maryland General Assembly
2007 Session

FISCAL AND POLICY NOTE

Senate Bill 514 (Senator Forehand)
Finance

Consumer Protection - Protection of Personal Information from Security Breaches

This bill requires businesses and State governmental entities that maintain personal information on State residents to notify individuals if the security of their information is breached and the personal information is disclosed or could potentially be disclosed to unauthorized persons. A business that does not comply with the provisions of this bill is guilty of an unfair or deceptive trade practice. In addition, an aggrieved person may bring an action against a person who violates the bill's provisions for damages and reasonable attorney's fees.

Fiscal Summary

State Effect: Potential significant. If security breaches occur, State agencies with large databases could incur expenditures for statewide media notification and additional personnel to investigate security breaches and provide assistance to affected individuals. State agencies with smaller databases could potentially incur significant expenditures for preparation and mailing of required notifications and assistance to affected individuals. Any cost recovery by the Attorney General from actions brought under the unfair and deceptive trade practices provision cannot be quantified beforehand.

Local Effect: None. The bill does not apply to counties or municipalities.

Small Business Effect: Potentially significant due to notification requirements and the impact from enforcement penalties and civil litigation costs if security breaches occur.

Analysis

Bill Summary: This bill requires businesses and State entities that own or license records that include personal information on State residents to notify those individuals of a security breach of the entity's information systems if, due to the breach, the individual's personal information has been acquired by an unauthorized person or is reasonably believed to have been acquired by an unauthorized person. Except as provided, State residents must be notified as soon as possible by the business or State entity after discovery of the security breach. If the business or State entity does not own the personal information subject to breach, then the owner or licensee of the personal information must be notified as soon as possible after discovery of the breach.

The notification of breach may be delayed if a law enforcement agency determines that notification will obstruct a criminal investigation or if the delay is necessary to determine the extent of the breach and restore system integrity. If notification is delayed due to a criminal investigation, then it must be provided as soon as possible after the law enforcement agency determines that notification will not obstruct the investigation.

The required notification to affected State residents may be given by written notice or electronic notice that meets the requirements of State law. A business or State entity may provide "substitute notice" under the following circumstances: • the cost of notifying individuals would exceed $250,000; • the affected class exceeds 500,000; or • the business or State entity does not have sufficient contact information.

If used, substitute notice must consist of • electronic mail if the business or State entity has an electronic mail address; • conspicuous posting on the Internet site if the business or State entity maintains a site; and • notification to major statewide media. A notice to an affected individual must include contact information for the business or State entity and a description of the categories of information acquired or believed to have been acquired by an unauthorized person.

A business or State entity subject to a security breach must notify the Office of the Attorney General within 24 hours after becoming aware of the breach. In addition, all national consumer reporting agencies that compile or maintain consumer credit information have to be notified if the breach requires notification to more than 5,000 individuals at one time.

A waiver of these notification provisions is void and unenforceable. In addition, businesses and State entities must comply with any other requirements for protection of personal information and privacy.

A violation is an unfair and deceptive trade practice and is subject to the enforcement and penalty provisions of the Maryland Consumer Protection Act. In addition, an aggrieved individual may bring an action against a person who violates these provisions to recover damages of $500 per violation or actual sustained damages, whichever is greater, and reasonable attorney's fees. Each individual failure to comply with the notification procedures under this bill is a separate violation.

Current Law: State law does not require notification to Maryland residents if the personal information owned, licensed, or maintained by a State governmental entity or a business is subject to a security breach and the personal information was disclosed or could have been disclosed to unauthorized persons.

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: • civil penalties of $1,000 for the first violation and $5,000 for subsequent violations; and • criminal sanction as a misdemeanor, with a fine of up to $1,000 and/or up to one year's imprisonment.

Background: The prospect of being victimized through the loss or theft of information held by data collection companies has captured national attention. ChoicePoint, a data collection company, exposed information on 163,000 consumers across the country through bogus business accounts that were set up by identity thieves. According to the Privacy Rights Clearinghouse, since disclosure of the ChoicePoint breach in February 2005, there have been at least 500 other known breaches of personal information records affecting over 104 million instances of Social Security numbers, driver's license numbers, and financial account numbers.

A number of states have enacted legislation to provide stronger consumer protections. It was a California law, enacted in 2002, requiring disclosure and notification of data breaches that forced ChoicePoint to reveal the compromise of its data. Since the ChoicePoint security breach, most states have considered notification legislation, including Maryland. According to the National Conference of State Legislatures, at least 35 states have enacted notification legislation. Breach notification legislation usually contains a "trigger" for notification of a breach. The trigger is based on risk or acquisition. State laws with a "risk" trigger generally require that notification be issued only if the breach reaches a defined level of risk that the data could be used to commit

identity fraud. The Arizona notification law is an example of a risk-based law. State laws using an "acquisition" trigger require that notification be issued to affected consumers regardless of the level of risk that the data could or could not be used to commit fraud. The California law is an example of an acquisition-based law. **Appendix 1** shows the states with security breach notification laws as of January 2007 and whether the laws are risk- or acquisition-based.

State Fiscal Effect: State general funds and special fund expenditures could potentially increase significantly under this bill in the event of a security breach that required the notification procedures. Many State agencies maintain personal information about millions of State citizens in their databases. The most obvious examples are the Comptroller of the Treasury, the Department of Health and Mental Hygiene, and the Motor Vehicle Administration. Other agencies that maintain extensive personal information on Maryland citizens include the Department of Human Resources; the Department of Labor, Licensing, and Regulation; the Department of Public Safety and Correctional Services; the University System of Maryland; the Department of Juvenile Services; and the Department of Housing and Community Development.

The State agencies that maintain personal information about 500,000 or more Maryland residents, or that could show that notification expenditures could exceed $250,000, would be authorized to provide "substitute notice." Substitute notice involves conspicuous notice on a web site, notification to major statewide media, and electronic mail notice to affected individuals, to the extent that the State entity has an electronic mail address. The costs of posting information regarding security breaches on web sites and notifying individuals by electronic mail (to the extent valid electronic mail addresses were available) could be absorbed within existing resources. The expenditures for notification to major statewide media could vary widely. "Major statewide media" is not defined in the bill, so agencies using substitute notice could notify newspapers and radio stations and issue press releases to meet the bill's requirements. This type of notification could probably be done within existing resources. However, it could be that State agencies using substitute notice would also have to purchase television and radio airtime and newspaper ads. Airtime and print ad expenditures could range from $30,000 to $300,000, per breach, depending on the types of ads purchased, since that is left to the discretion of the State agency.

If a security breach affected separate databases within a State agency or affected smaller State agencies or offices that held personal information on less than 500,000 individuals, or if the cost of notification would not exceed $250,000, then the State entity would be required to notify affected individuals by written notice or electronic mail. The electronic notice would have to meet federal standards for sufficiency. To the extent that these State entities could notify affected individuals by electronic mail, those expenditures

could be absorbed within existing resources. However, since State entities may or may not have valid e-mail addresses in their personal information records, it is also likely that they would have to provide written notice. Expenditures could range from $100,000 to $250,000 for State entities with personal information on less than 500,000 individuals. In addition to mailing costs, these entities would probably have to hire temporary contractual assistance to prepare and send out notifications and provide assistance to affected individuals.

All State agencies subject to a security breach could incur additional expenditures for computer programming vendors to investigate and repair computer programs affected by a security breach. In addition, some larger State agencies could need to hire additional customer service personnel on a temporary basis to manage phone inquiries from affected individuals.

Small Business Effect: There could be a significant impact on those small businesses that maintain personal information databases if subject to a security breach. Small businesses with databases of less than 500,000 or that could not show that notification costs would exceed $250,000 would be required to notify affected individuals of a security breach by written notification or electronic mail. Electronic mail notification could be provided without significant additional cost to these businesses, but that would apply only to the extent that businesses have valid e-mail addresses. Small businesses that are required to provide written notice under the provisions of this bill could incur significant costs for additional personnel and supplies for the preparation and mailing of written notices.

For those small businesses that could demonstrate that they did not have sufficient contact information for the affected individuals, they could provide substitute notice. The businesses would be required to notify affected individuals by electronic mail or through conspicuous web site posting only if the businesses have electronic e-mail addresses or maintain web sites. They would, in any event, be required to notify major statewide media. While this could be limited to notification of radio stations and newspapers, it could also likely involve the purchase or air and print time for notification. Some small businesses may find it less costly to set up a web site in the event of a security breach, rather than pay for television and radio advertising time.

Small businesses could be subject to potentially significant costs in the event they are charged with unfair and deceptive trade practices, and are subject to enforcement penalties and civil litigation as a result of security breaches.

Additional Comment: Encryption of databases with personal information is not required under the provisions of this bill, nor are State entities or businesses required to

limit employee access to personal information. However, passage of this bill could result in State entities and businesses expending additional funds to encrypt databases that are not already encrypted and they could take additional steps to limit access to personal information and supervise those employees with authorized access to avoid the expenditures that would be required in the event of a security breach.

Additional Information

Prior Introductions: This bill is a reintroduction of HB 873 of 2006, which was referred to the House Economic Matters Committee but then withdrawn.

Cross File: None.

Information Source(s): Department of Human Resources; Department of Health and Mental Hygiene; Maryland Department of Transportation; Department of Labor, Licensing, and Regulation; Department of Budget and Management; Office of the Attorney General (Consumer Protection Division); U.S. PIRG; State PIRG; Privacy Rights Clearinghouse; National Conference of State Legislatures; Department of Legislative Services

Fiscal Note History: First Reader - February 26, 2007
mll/jr

Analysis by: Karen D. Morgan

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

Appendix 1
Security Breach Notification /State Laws

State	Notification Basis*	Comments
Arizona	Risk	
Arkansas	Risk	
California	Acquisition	
Colorado	Risk	
Connecticut	Risk	
Delaware	Acquisition	
Florida	Acquisition	
Georgia	Acquisition	Applies to data brokers only
Hawaii	Acquisition	
Idaho	Risk	
Illinois	Acquisition	
Indiana	Acquisition	Applies to state agencies only
Kansas	Risk	
Louisiana	Risk	
Maine	Acquisition	Applies to information brokers only
Michigan	Risk	
Minnesota	Acquisition	Excludes health information and financial entities
Montana	Risk	
Nebraska	Risk	
Nevada	Acquisition	
New Hampshire	Risk	
New Jersey	Risk	
New York	Acquisition	
North Carolina	Risk	
North Dakota	Acquisition	
Ohio	Risk	
Oklahoma	Acquisition	Applies to state agencies only
Pennsylvania	Risk	
Rhode Island	Acquisition	Excludes health information entities
Tennessee	Acquisition	
Texas	Acquisition	
Utah	Risk	
Vermont	Risk	
Washington	Risk	
Wisconsin	Risk	

*Eighteen states use a “risk-based” notification trigger and 17 states use an “acquisition-based” trigger.
Source: National Conference of State Legislatures; State Public Interest Research Groups