Legislative Analysis

Mitchell Bean, Director
Phone: (517) 373-8080
http://www.house.mi.gov/hfa

DATABASE SECURITY BREACH: NOTIFY STATE RESIDENTS

Senate Bill 309 (Substitute H-3)
Sponsor: Sen. Shirley Johnson
House Committee: Banking and Financial Institutions
Senate Committee: Banking and Financial Institutions

First Analysis (12-5-06)

BRIEF SUMMARY: The bill would require entities to notify affected state residents when the security of a database containing personal information maintained by that entity was breached; create a protocol for the notification; provide exemptions to the notification requirements; and create both criminal and civil penalties for violations of the bill.

FISCAL IMPACT: The bill would have an impact on state and local governments. For a more detailed fiscal analysis, see below.

THE APPARENT PROBLEM:

In October of 2004, ChoicePoint, a national data aggregating company, had the personal information of 145,000 individuals nationwide stolen from its database. However, the company did not report the theft of the information until four months later, leaving plenty of time for identify thieves to use the information to ruin the credit of the victims. Since that time, at least 35 states have enacted legislation requiring companies that maintain databases of personal information to notify affected residents in their states in a timely manner if the security of a database was compromised. Michigan has no such requirement.

THE CONTENT OF THE BILL:

The bill would amend the Identity Theft Protection Act. In the event of a security breach of a database containing personal information, the bill would require a state agency (including a college or university), an individual, or a business to notify, without reasonable delay, each Michigan resident for whom personal information had been maintained in the database by that entity. The bill would take effect 180 days after enactment. Among other things, the bill would do the following.

- Require an entity to notify residents when a breach occurs unless the breach is determined not to cause or likely not to cause substantial loss or injury to, or result in identity theft in regards to, one or more state residents. Such a determination would be based on the prudent person standard.

- Define "breach of the security of a database" or "security breach" to mean the unauthorized access and acquisition of computerized personal information that

compromises the security or confidentiality of personal information maintained by an entity as part of a database of personal information. These terms would not apply to unauthorized access by an employee or other individual if the person had acted in good faith in accessing the data; the access related to the activities of the entity; and the employee or other individual did not misuse or disclose any of the information to an unauthorized person or business.

- Define "personal information" to include the first name or first initial plus the last name linked to a social security number; driver license or state ID number; and/or bank account or credit or debit card number along with a security code, access code, or password allowing access to a resident's financial accounts.

- Require the notices of the breach to those residents whose unencrypted and unredacted personal information was accessed and acquired by an unauthorized person and also to those whose information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key. "Encrypted" refers to securing information so that the data elements are unreadable or unusable, or transforming the data through an algorithmic process so that it is unlikely a meaning could be assigned without use of a key to decode it. "Redact" would mean to alter or truncate data so that no more than the last four sequential digits of a driver license, state ID, or account number, or no more than five sequential digits of a Social Security number, would be accessible as part of personal information.

- Prescribe several allowable formats for the notices, including email, and specify the information to be included in the notice.

- Provide an alternate means of providing the required notices if the cost of complying would exceed $250,000 or if more than 500,000 people would have to be noticed.

- Require, in some instances, the entity to notify the national consumer reporting agencies (e.g., Experion).

- Specify that financial institutions subject to federal oversight, and entities subject to and in compliance with the Health Insurance Portability and Accountability Act (HIPAA), would be considered to be in compliance with the bill's provisions.

- Specify the manner in which a public utility that experienced a security breach would have to notify its customers.

- Establish criminal and civil penalties for certain actions and inactions.

Penalties

Providing notice of a security breach when one hadn't occurred, with intent to defraud, would be a misdemeanor punishable by imprisonment for not more than 30 days and/or a penal fine of not more than $250. A person that knowingly failed to provide a required notice of a security breach could be ordered to pay a civil fine of not more than $250 for each failure to provide notice. ("Person" is defined in the act to mean an individual, partnership, corporation, limited liability company, association, or other legal entity.)

An action to recover a civil fine could be brought by the attorney general or a prosecuting attorney. A person's liability for civil fines would be capped at $750,000 for multiple violations of the above arising from the same security breach. These penalties would apply to the discovery or notification of a breach occurring on or after the bill's effective date. In addition, these provisions would preempt any charter, ordinance, resolution, regulation, rule, or other action by a local unit of government.

Data containing personal information must be destroyed when removed from the database and the entity is no longer retaining the data elsewhere for another lawful purpose, though the data could be retained for purposes of an investigation, audit, or internal review. A person who knowingly violated this provision would be guilty of a misdemeanor punishable by a penal fine of not more than $250 for each violation.

A person also could not distribute an advertisement or make any solicitation that misrepresented to the recipient that a security breach had occurred that could affect the recipient or one that was substantially similar to a notice required under the bill or by federal law, if the form of the notice had been prescribed by state or federal law, rule, or regulation. A person who knowingly or intentionally violated this provision would be guilty of a misdemeanor punishable by not more than 30 days' imprisonment and/or a penal fine of not more than $1,000 for each violation.

None of the above criminal penalties would affect the availability of any civil remedy for a violation of those provisions or any other state or federal law.

MCL 445.63 et al.

HOUSE COMMITTEE ACTION:

The committee substitute made several changes considered to be technical in nature. Substantive changes included lowering the maximum civil fine and two of the penal fine amounts to $250; lowering the aggregate civil liability to $750,000 (from $2.5 million); eliminating jail time for failure to destroy data as required and eliminating the element of intent from that crime; exempting access or acquisition of governmental documents lawfully available to the general public from the bill's provisions; and revising the definition of "redact" to allow entities to block the last four digits of a Social Security number from public disclosure.

FISCAL INFORMATION:

The bill would increase local government revenue and expenditures by an indeterminate amount. Local expenditures would increase to cover the cost of misdemeanor probation and jail, which vary by county. In addition, the bill provides for civil actions by individuals, which would also increase local court costs. The criminal fines provided in the bill should qualify as penal fine revenue and would benefit public libraries. It is not clear where the $250 civil fine is to be deposited. Revenue and expenditures estimates would depend on the number of security breaches for which proper notification is not provided, an amount not currently determinable.

ARGUMENTS:

For:

The bill would require state agencies, local governments, and businesses to notify Michigan residents if their personal information has been stolen through a database security breach. Such personal information can be used to access a person's medical records and financial accounts, and by identity thieves to open up new accounts in the person's name. The bill would place the burden on a business to make a determination that the breach had not or would not cause substantial loss or injury to, or result in identify theft with respect to, one or more state residents, yet would not be overly burdensome. There are several exemptions to the required notifications, and, if the breach affected over a half million or would cost over a quarter of a million dollars to notify all affected individuals, a company could use mass media, such as television advertisements, to notify residents. In addition, though the bill contains one of the highest criminal and civil fine penalty clauses in the nation, it would still cap the civil fine at a level that should not bankrupt a company. Though the criminal fines for failing to destroy data as required under the bill and provided a fraudulent notice of a security breach were reduced from the Senate-passed version, the penalty for knowingly and intentionally distributing advertisements or other solicitations similar to the notices required for a legitimate security breach would remain as a 30-day misdemeanor and possible fine of up to $1,000 to deter criminals from phishing or otherwise attempting to lure state residents into giving up personal information that could be used in identity theft.

The bill does not specify a set time frame that a company or governmental agency must provide the required notification, but they must do so without reasonable delay; this is a standard commonly used in federal law and also used by the states with similar legislation on security breach notifications. Another strength of the bill is that it would protect the last four digits of a person's Social Security number (SSN) by allowing companies and agencies to redact (black out) those digits and use the first five digits in documents. This is important because SSNs are different from credit or bank account numbers; it the last four digits of an SSN that is unique to an individual (the other numbers refer to the state of issue and the year of issue) whereas the last four numbers of a credit card are the least sensitive or personally identifiable.

The bill is good public policy and represents a collaborative effort between consumer protection groups and businesses and is widely supported.

Response:

The use of "person" in the penalty provisions may be problematic. A closer look at how the bill's definition of "agency," which would include state employees, interacts with the act's current definition of "person" deserves a closer look to ensure that the bill – by specifying that a "person" who violated the bill's provisions would be subject to its penalties – would not inadvertently shield state employees from criminal prosecution or civil fine liability.

In addition, if the maximum term of imprisonment for knowingly and intentionally distributing fake security breach notices in an effort to solicit personal information was increased to 93-days, certain fingerprint and record keeping requirements would be triggered, including a fingerprint check of the FBI database, that would enable law enforcement to track repeat offenders.

POSITIONS:

The Public Interest Research Group in Michigan (PIRGIM) supports the bill. (12-5-6)

AARP of Michigan supports the bill. (12-5-06)

Michigan Association of Health Plans indicated support for the bill. (12-5-06)

Insurance Institute of Michigan indicated support for the bill. (12-5-06)

Michigan Health and Hospital Association indicated support for the bill. (12-5-06)

Trinity Health/Care Choices indicated support for the bill. (12-5-06)

Michigan Bankers Association indicated support for the bill. (12-5-06)

Lexis Nexis indicated neutrality on the bill. (12-5-06)

Legislative Analyst: Susan Stutzky
Fiscal Analyst: Richard Child

■ This analysis was prepared by nonpartisan House staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.