Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986
TDD: (517) 373-0543

Senate Bill 309 (as enrolled) **PUBLIC ACT 566 of 2006**
Sponsor: Senator Shirley Johnson
Senate Committee: Judiciary
House Committee: Banking and Financial Services

Date Completed: 1-19-07

CONTENT

The bill amends the Identity Theft Protection Act to do all of the following:

-- Require a person or State agency that owns or licenses data included in a database to notify Michigan residents if an unauthorized person gained access to or acquired their personal information.
-- Require a person or agency that maintains a database to give notice of a security breach to the owner or licensor of information in the database.
-- Require that notification be provided without unreasonable delay, except in certain circumstances.
-- Specify several methods by which notice may be given.
-- Require a person or agency who notifies Michigan residents of a security breach also to notify consumer reporting agencies, except under certain circumstances.
-- Prescribe criminal penalties and civil remedies for failing to provide a required notice, falsely providing notice, and misrepresenting that a security breach has occurred.
-- Permit any local action to regulate any matter addressed by the bill's notification requirements.
-- Require the destruction of data containing personal information when that data are removed from a database and not retained elsewhere for a lawful purpose.

The bill will take effect on July 2, 2007.

Notice Requirement

The bill requires a person or agency that owns or licenses data included in a database to notify each resident of Michigan to whom one or both of the following apply, if the person or agency discovers a security breach or receives notice of a security breach from a person or agency that maintains the database:

-- An unauthorized person gained access to or acquired the resident's unencrypted and unredacted personal information.
-- A person with unauthorized access to the encryption key gained access to or acquired the resident's personal information.

Also, if a person or agency maintains a database that includes data the person or agency does not own, and discovers a security breach, the person or agency must give notice of the breach to the owner or licensor of the information.

The notification requirements apply unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of Michigan. In making this determination, the person or agency must act with the care an ordinarily prudent person or agency in a like position would exercise under similar circumstances.

Under the Act, "person" means an individual, partnership, corporation, limited liability company, association, or other legal

entity. Under the bill, "agency" means a department, board, commission, office, agency, authority, or other unit of State government. The term includes an institution of higher education of this State, but does not include a circuit, probate, district, or municipal court.

The bill defines "personal information" as the first name or first initial and last name linked to one or more of the following data elements of a Michigan resident:

-- Social Security number.
-- Driver license number or State personal identification card number.
-- Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.

"Breach of security of a database" or "security breach" means the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals. These terms do not include unauthorized access to data by an employee or other individual if the access meets all of the following:

-- The employee or other individual acted in good faith in gaining access to the data.
-- The access was related to the activities of the agency or person.
-- The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person.

"Data" means computerized personal information. "Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable. "Redact" means to alter or truncate data so that no more than four sequential digits of a driver license number, State personal identification card number, or account number, or no more than five sequential digits of a Social Security number, are accessible as part of personal information.

Delay in Providing Notice

A person or agency required to provide notice under the bill must provide it without unreasonable delay. A person or agency may delay providing notice without violating this provision, however, if either of the following applies:

-- A delay is necessary for the person or agency to take any measures necessary to determine the scope of the breach and restore the reasonable integrity of the database.
-- A law enforcement agency determines and advises the agency or person that providing notice will impede a criminal or civil investigation or jeopardize homeland or national security.

In the event of such a delay, the person or agency must provide the required notice without unreasonable delay after completing the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database or after the law enforcement agency determines that providing the notice will no longer impede an investigation or jeopardize homeland or national security.

Providing Notice

The bill specifies several methods by which an agency or person may provide a required notice. The agency or person may provide written notice sent to the recipient's postal address in the agency's or person's records. Written notice also may be sent electronically to the recipient if any of the following apply:

-- The recipient has expressly consented to receive electronic notice.
-- The person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications and, based on those communications, the person or agency reasonably believes that it has the recipient's current electronic mail address.
-- The person or agency conducts its business primarily through internet account transactions or on the internet.

If not otherwise prohibited by State or Federal law, an individual representing the person or agency may give notice by telephone if the notice is not given in whole or in part by use of a recorded message and the recipient has expressly consented to receive notice by telephone. If the recipient has not given express consent, the person or agency also must provide written or electronic notice if the notice by telephone does not result in a live conversation between the person's or agency's representative and the recipient within three business days after the initial attempt to telephone the recipient.

The person or agency may provide substitute notice, if it demonstrates that the cost of providing any notice described above will exceed $250,000 or that the person or agency has to provide notice to more than 500,000 Michigan residents. A person or agency provides substitute notice by doing all of the following:

-- Providing electronic notice to Michigan residents, if the person or agency has electronic mail addresses for any of those residents who are entitled to receive the notice.
-- Conspicuously posting the notice on the person's or agency's website, if the person or agency maintains a website.
-- Notifying major statewide media.

Media notification must include a telephone number or a website address that a person may use to obtain additional assistance and information.

A written notice sent by mail or electronically must be written in a clear and conspicuous manner and contain the content listed below. Notice provided by telephone must clearly communicate the same content to the recipient of the call. A notice provided under the bill must do all of the following:

-- Describe the security breach in general terms.
-- Describe the type of personal information that is the subject of the unauthorized access or use.
-- Generally describe what the agency or person providing the notice has done to protect data from further security breaches, if applicable.
-- Include a telephone number where a notice recipient may obtain assistance or additional information.
-- Remind recipients of the need to remain vigilant for incidents of fraud and identity theft.

A public utility that sends monthly billing or account statements to the postal address of its customers may provide notice of a security breach to its customers in the manner described above or by providing all of the following:

-- Electronic notice, as described above.
-- Notification to the media reasonably calculated to inform the public utility's customers of the security breach.
-- Conspicuous posting of the notice on the utility's website.
-- Written notice sent in conjunction with the monthly billing or account statement to the customer at the customer's postal address in the utility's records.

A person or agency may provide any notice required under the bill pursuant to an agreement between that person or agency and another person or agency, if the notice provided pursuant to the agreement does not conflict with any provision of the bill.

After providing a notice described above, the person or agency must provide notice of the security breach, without unreasonable delay, to each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis. This notification must include the number of notices that the person or agency provided to Michigan residents and the timing of those notices. These requirements do not apply if either of the following is met:

-- The person or agency is required under the bill to provide notice of a security breach to 1,000 or fewer Michigan residents.
-- The person or agency is subject to Title V of the Federal Gramm-Leach-Bliley Act (15 USC 6801-6809) (which deals with the protection and disclosure of nonpublic personal information by financial institutions).

A financial institution is considered to be in compliance with the bill's notification requirements if it is subject to, and has notification procedures for compliance with,

response guidance programs and customer notice requirements prescribed by the board of governors of the Federal Reserve System and the other Federal bank and thrift regulatory agencies, or similar guidance prescribed and adopted by the National Credit Union Administration and its affiliates.

A person or agency is considered to be in compliance with the bill's notification requirements if it is subject to and in compliance with the Federal Health Insurance Portability and Accountability Act (HIPAA), and with regulations promulgated under that Act for the prevention of unauthorized access to customer information and customer notice.

Notice Violations; Advertisement; Solicitation

A person who knowingly fails to provide any notice of a security breach required under the bill may be ordered to pay a civil fine of up to $250 for each failure to provide notice. The Attorney General or a prosecuting attorney may bring an action to recover a civil fine. A person's maximum aggregate liability for multiple violations that arise from the same security breach is $750,000.

Providing notice of a security breach in a manner described in the bill when a security breach has not occurred, with the intent to defraud, is a misdemeanor punishable by up to 30 days' imprisonment or a maximum fine of $250 for each violation, or both.

In addition, the bill prohibits a person from distributing an advertisement or making any other solicitation that misrepresents to the recipient that a security breach that may affect the recipient has occurred. The bill also prohibits a person from distributing an advertisement or making any other solicitation that is substantially similar to a security breach notice required under the bill or by Federal law, if the form of that notice is prescribed by State or Federal law, rule, or regulation. A person who knowingly or intentionally violates either prohibition is guilty of a misdemeanor punishable by up to 30 days' imprisonment or a maximum fine of $1,000 for each violation, or both.

None of the penalty provisions described above affects the availability of any civil remedy for a violation of the provisions or any other State or Federal law.

Destruction of Data

The bill requires a person or agency that maintains a database that includes personal information regarding multiple individuals to destroy any data that contain personal information concerning an individual when such data are removed from the database and are not retained elsewhere for another purpose not prohibited by State or Federal law. This provision does not prohibit a person or agency from retaining data that contain personal information for purposes of an investigation, audit, or internal review.

A knowing violation is a misdemeanor punishable by a maximum fine of $250 for each violation. This penalty does not affect the availability of any civil remedy for a violation of State or Federal law.

A person or agency is considered to be in compliance with this data destruction requirement if the person or agency is subject to and in compliance with Federal law concerning the disposal of records containing personal identifying information.

The bill defines "destroy" as to destroy or arrange for the destruction of data by shredding, erasing, or otherwise modifying the data so that they cannot be read, deciphered, or reconstructed through generally available means.

Scope of Notification Requirements

The bill's notification requirements apply to the discovery or notification of a breach of the security of a database occurring on or after the bill's effective date. Those requirements do not apply to the access or acquisition by a person or agency of Federal, State, or local government records or documents lawfully made available to the general public.

The bill also provides that its notification requirements deal with subject matter that is of statewide concern, and any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of the State to regulate any matter expressly set forth in those requirements is preempted.

MCL 445.63 et al.

Legislative Analyst: Patrick Affholter

FISCAL IMPACT

The bill will have an indeterminate fiscal impact on State and local government.

Costs to the State will depend on the number of security breaches that occur in the future.

There are no data to indicate how many offenders will be convicted of violating the bill. Local units will incur the costs of misdemeanor probation and incarceration in a local facility, both of which vary by county. Public libraries will benefit from any additional penal fine revenue.

The bill will have an indeterminate impact on the Department of Information Technology. The costs incurred will depend on the number and size of security breaches requiring notification under the bill.

Fiscal Analyst: Lindsay Hollander
Stephanie Yu

S0506\s309es