# Legislative Analysis

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

**DATABASE SECURITY BREACH:**
**NOTIFY STATE RESIDENTS**

**Senate Bill 309**
**Sponsor: Sen. Shirley Johnson**
**House Committee: Banking and Financial Institutions**
**Senate Committee: Banking and Financial Institutions**

**Complete to 12-4-05**

**A SUMMARY OF SENATE BILL 309 AS PASSED BY THE SENATE 11-30-06**

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. Among other things, the bill would do the following.

- Apply the notice requirements only to breaches determined to cause or likely 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 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.

- 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 $1,000. A person that failed to provide a required notice of a security breach could be ordered to pay a civil fine of not more than $1,000 for each failure to provide notice.

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 $2.5 million 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 or intentionally violated this provision would be guilty of a misdemeanor punishable by not more than 30 days imprisonment and/or a fine of not more than $1,000 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 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.

**FISCAL IMPACT:**

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 $1,000 criminal fine provided in the bill should qualify as penal fine revenue and would benefit public libraries. It is not clear where the $1,000 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.

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.