



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 introduced 3-16-05)
Sponsor: Senator Shirley Johnson
Committee: Judiciary

Date Completed: 5-2-05

CONTENT

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

- Require a State agency, or a person doing business in Michigan, that owned or licensed computerized data that included personal identifying information, to notify a Michigan resident whose information was acquired, or whose information the agency or person reasonably believed was acquired, by an unauthorized person.**
- Require an agency, or a person doing business in Michigan, that maintained computerized data including personal identifying information to notify the information's owner or licensee of a breach in the data's security, if personal identifying information were acquired, or the agency or person reasonably believed it was acquired, by an unauthorized person.**
- Specify that an agency or person required to give notice under the bill also would have to notify the Department of Attorney General, the Department of State Police, and a local law enforcement agency.**
- Include failure to give the required notice in the Act's list of prohibited activities in the conduct of trade or commerce.**
- Specify civil remedies for a person injured by a violation of the bill.**

Notice

Under the bill, an agency of this State, or a person doing business in Michigan, that owned or licensed computerized data that included personal identifying information, would have to provide notice of any breach of the security of the system, following discovery or notification of the breach, to a Michigan resident whose unencrypted personal identifying information was acquired by an unauthorized person or if the agency or person reasonably believed that an unauthorized person had acquired that information. The agency or person would have to provide notice in the most expedient time possible and without unreasonable delay unless, in the case of a person doing business in Michigan, delay were necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

An agency, or a person doing business in Michigan, that maintained computerized data that included personal identifying information that the agency or person did not own, would have to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal identifying information were acquired by an unauthorized person or if the agency or person reasonably believed that an unauthorized person had acquired that information.

An agency or person doing business in Michigan could provide the required notice either by written notice, or by electronic notice if it were consistent with the provisions regarding electronic records and signatures established in Section 101 of Title I of the Federal Electronic Signatures in Global and National Commerce Act (15 USC 7001), and the agency or person did not have sufficient contact information for the individuals, owners, or licensees to provide each with written notice.

An agency or a person doing business in Michigan that was required to provide notice under the bill also would have to notify the Department of Attorney General, the computer crimes section of the Department of State Police, and any local law enforcement agency with jurisdiction in the city, village, or township where the agency or person was located.

Under the bill, "agency" would mean a department, board, commission, office, agency, authority, or other unit of State government, and would include a State institution of higher education.

"Breach of the security of the system" would mean the unauthorized acquisition of computerized data that compromised the security, confidentiality, or integrity of personal identifying information maintained by an agency or a person doing business in Michigan. It would not include good faith acquisition of personal identifying information by an agency's or person's employee or agent related to the agency's or person's activities, if the personal identifying information were not used or subject to further unauthorized disclosure.

Under the Act, "personal identifying information" means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including a person's name, address, telephone number, driver license or State personal identification card number, Social Security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.

Trade or Commerce

The Act prohibits a person from doing certain things in the conduct of trade or commerce. A knowing or intentional violation is a misdemeanor punishable by up to 30 days' imprisonment and/or a maximum fine of \$1,000. The criminal penalty does not affect the availability of any civil remedy. The bill would include failing to provide notice to a person of a breach of the security of a data system in the Act's list of prohibited activities in the conduct of trade or commerce.

Civil Remedies

A person injured by a violation of the bill could bring a civil action to recover actual damages and reasonable attorney fees, or seek injunctive or any other relief available at law or in equity.

MCL 445.71 et al.

Legislative Analyst: Patrick Affholter

FISCAL IMPACT

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

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

There are no data to indicate how many offenders would be convicted of failing to provide notice of a security breach. Local units would incur the costs of misdemeanor probation and incarceration in a local facility, both of which vary by county. Public libraries would benefit from any additional penal fine revenue. The bill also could increase costs to local courts by allowing persons injured by a violation of the proposed section to initiate a civil action.

Fiscal Analyst: Bill Bowerman
Bethany Wicksall

S0506\sb309sa

This analysis was prepared by nonpartisan Senate staff for use by the Senate in its deliberations and does not constitute an official statement of legislative intent.