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

BILL ANALYSIS

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

House Bill 6405 (Substitute S-1 as reported)
House Bill 6406 (Substitute S-1 as reported)
Sponsor: Representative Diana Farrington (H.B. 6405)
Representative Joseph Graves (H.B. 6406
House Committee: Financial Services
Senate Committee: Finance

CONTENT

House Bill 6405 (S-1) would enact the "Data Breach Notification Act", which would do the following:

-- Require each covered entity and third-party agent to implement and maintain reasonable security measures designed to protect sensitive personally identifying information against a breach of security.
-- Require a covered entity to conduct a good-faith and prompt investigation if it determined that a breach of security had or could have occurred.
-- Require a covered entity or third-party agent to provide notice of a breach to each State resident whose sensitive personally identifiable information was acquired in the breach if the entity that owned or licensed the information determined that a breach had occurred.
-- Require a covered entity that used a credit card payment processor or a credit card payment gateway in the conduct of its business to provide notice within 45 days of its determination that a breach had occurred.
-- Require a covered entity that did not use a credit card payment processor or a credit card payment gateway in the conduct of its business to provide notice within 75 days of its determination that a breach had occurred.
-- Require a covered entity to provide notice to a State resident in compliance with certain criteria listed under the proposed Act.
-- Require a covered entity to provide written notice of the breach to the Department of Technology, Management, and Budget (DTMB) if the number of State residents the covered entity was required to notify exceeded 750, and prescribe the contents of the notice.
-- Require a covered entity also to notify certain consumer reporting agencies if an entity discovered circumstances that required it provide notice to more than 1,000 State residents at a single time.
-- Require a third-party agent who experienced a breach of security in a system it maintained to notify the covered entity of the breach of security as quickly as practicable.
-- Prescribe civil fines for a knowing violation of a notification requirement.
-- Subject State agencies to the notice requirements of the bill.
-- Require the DTMB, by February 1 of each year, to submit a report to certain government officials that described the nature of any reported breaches of security by State agencies or their third-party agents in the preceding calendar year along with recommendations for security improvements.
-- Require a covered entity or third-party agent to take reasonable measures to dispose of information within its custody or control when its retention was no longer required.

-- Specify that certain notification provisions would preempt any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of the State to regulate those matters.

House Bill 6406 (S-1) would amend the Identity Theft Protection Act to do the following:

-- Specify that an entity that was subject to or regulated under the Insurance Code would be exempt from the Act.
-- Specify that an entity that owned, was owned by, or was under common ownership with an entity described above, and maintained the same cybersecurity procedures as that entity, would be exempt from the Act.
-- Delete various definitions from the Act.

The bill also would repeal Sections 12, 12a, and 12b of the Identity Theft Protection Act.

MCL 445.63 et al. (H.B. 6406) Legislative Analyst: Drew Krogulecki

FISCAL IMPACT

The bills would have an impact on the Department of Technology, Management, and Budget (DTMB) as the collection point for notifications affecting 750 or more State residents of an estimated $250,000, of which $50,000 would be an annual cost. The Department has indicated that the cost to create a new website so that it could intake the required information in the case of a breach involving 750 or more residents is estimated at $200,000. Additionally, the annual cost for the Department to host the information and provide support is estimated at $50,000 annually. The Department also has indicated that additional, indeterminate costs could be incurred in the future depending on the number of notifications received by the DTMB and any requirements for further dissemination of that information to government and/or private sector entities.

The $250,000 estimated additional cost for the DTMB would be in addition to already appropriated funds spent on homeland and cyber security. Since fiscal year (FY) 2014-15, and through the end of FY 2017-18, the DTMB has spent an estimated $46.5 million on building, maintaining, and expanding homeland and cyber security to protect the State's entire data system. That funding is used by the Michigan Security Operations Center (MiSOC), which is responsible for identifying, managing, and mitigating information security risks and vulnerabilities within the State of Michigan government computing, communication, and technology resources. The MiSOC also assists all State agencies with their security issues, enforcement oversight of State security policies, and procedures intended to maintain suitable levels of enterprise-wide security.

The State also provides continuing statewide support for the prevention, response, and recovery of data that has been breached, including law enforcement investigation efforts, though major breach investigations would garner immediate investigations by the Secret Service and the FBI. The Department of State Police's (MSP) Michigan Intelligence Operations Center (often referred to as fusion center) serves as an interagency coordinating clearinghouse and provides 24-hours-a-day, statewide information sharing among local, State, and Federal public safety agencies and private sector organizations in order to facilitate the collection, analysis, and dissemination of intelligence relevant to cyber security incidents and other emergencies. The MSP's Michigan Cyber Command Center works with the DTMB and others to coordinate combined efforts of cyber emergency response during critical cyber incidents, and also works with public and private entities to provide advice on best practices to ensure data security.

Schools and local governments that own or license personally identifying information would experience additional costs for implementing and maintaining reasonable security measures and for House Bill 6405's notification requirements.

Regarding the civil fines for violations of the Act, the bills would create an indeterminate fiscal impact on the State and local government. House Bill 6406 (S-1) would eliminate misdemeanor offenses for violations of the Identity Theft Protection Act related to misrepresenting security breaches and failing to destroy personal information once the information has been removed from a database. To the extent that changes in the bill led to decreased misdemeanor arrests and prosecutions, it could reduce resource demands on law enforcement, court systems, and jails.

The bills would change the application and amounts of civil fines for violations of the Act. Civil fines for notification requirement violations would range from $2,000 per violation up to a $5,000-per-day cap for consecutive violations. The aggregate civil fine liability from the same security breach under the bills would be capped at $250,000, a reduction from the $750,000 cap under current law. Any change in civil fine revenue would depend on the number and extent of violations of the Act.

Date Completed: 12-17-18

Fiscal Analyst: Bruce Baker
Ryan Bergan
Joe Carrasco
Abbey Frazier
Cory Savino