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 H-3 as passed by the House)
House Bill 6406 (Substitute H-1 as passed by the House)
Sponsor: Representative Diana Farrington
Representative Joseph Graves
House Committee: Financial Services
Senate Committee: Finance

Date Completed: 12-13-18

CONTENT

House Bill 6405 (H-3) 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 a covered entity determined that a breach of security had or could have occurred.
-- Require a covered entity 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 to provide notice within 45 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 sensitive personally identifying information within its custody or control when its retention was no longer required.

House Bill 6406 (H-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.
-- Delete various definitions from the Act.

The bill also would repeal Sections 12, 12a, and 12b of the Identity Theft Protection Act. (Section 12 requires, under certain circumstances, a person or agency that owns or licenses data that are included in a database that discovers a security breach to provide a notice of the breach to each resident of the State who meets certain criteria, and includes further data breach notice procedures, among other things. Section 12a 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 that data are removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by State or Federal law.

Section 12b prohibits a person from distributing an advertisement or making any other solicitation that misrepresents to the recipient that a security breach has occurred that may affect the recipient, among other things.)

The bills are tie-barred. Also, House Bill 6405 (H-3) is tie-barred to House Bill 6491 (which would create Chapter 5A (Data Security) under the Insurance Code). Each bill would take effect 90 days after its enactment.

House Bill 6405 (H-3) is described in further detail below.

House Bill 6405 (H-3)

Definitions

Under the bill, "breach of security" or "breach" would mean the unauthorized acquisition of sensitive personally identifying information in electronic form, if that acquisition is reasonably likely to cause substantial risk of identity theft or fraud to the State residents to whom the information relates. Acquisition that occurred over a period of time that was committed by the same entity would constitute one breach. The term would not include any of the following:

-- A good-faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information was used for a purpose unrelated to the business of the covered entity or was subject to further unauthorized use.
-- A release of a public record that was not otherwise subject to confidentiality or nondisclosure requirements.
-- An acquisition or release of data in connection with a lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the State or a political subdivision of the State.

Except as provided below, "sensitive personally identifying information" would mean a State resident's first name or first initial and last name in combination with one or more of the following data elements that relate to that State resident:

-- A nontruncated Social Security number.

-- A nontruncated driver license number, State personal identification card number, passport number, military identification number, or other unique identification number issued on a government document that is used to verify the identity of a specific individual.
-- A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will result in a credit or debit to the financial account.
-- A State resident's medical or mental history, treatment, or diagnosis issued by a health care professional.
-- A State resident's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the state resident.
-- A username or electronic mail (e-mail) address, in combination with a password or security question and answer, that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

"Sensitive personally identifying information" would not include any of the following:

-- Information about a state resident that had been lawfully made public by a Federal, State, or local government record or a widely distributed media.
-- Information that was truncated, encrypted, secured, or modified by any other method or technology that removed elements that personally identified a State resident or that otherwise rendered the information unusable, including encryption of the data or device containing the sensitive personally identifying information, unless the covered entity knew or reasonably believed that the encryption key or security credential that could render the personally identifying information readable or usable had been breached together with the information.

"Covered entity" would mean an individual or a sole proprietorship, partnership, government entity, corporation, limited liability company, nonprofit, trust, estate, cooperative association, or other business entity, that owns or licenses sensitive personally identifying information. The term also includes a State agency.

"Data in electronic form" would mean any data that is stored electronically or digitally on any computer system or other database, including, but not limited to, recordable tapes and other mass storage devices.

"State agency" would mean an agency, board, bureau, commission, department, division, or office of the State that owns, acquires, maintains, stores, or uses data in electronic form that contains sensitive personally identifiable information.

"Third-party agent" would mean an entity that maintains, processes, or is otherwise permitted to access, sensitive personally identifying information in connection with providing services to a covered entity under an agreement with the covered entity.

Security Measures

Each covered entity and third-party agent would have to implement and maintain reasonable security measures designed to protect sensitive personally identifying information against a breach of security.

A covered entity would have to consider all of the following in developing its reasonable security measures:

-- The size of the covered entity.
-- The amount of sensitive personally identifying information that was owned or licensed by the covered entity and the type of activities for which the information was accessed, acquired, or maintained by or on behalf of the covered entity.
-- The covered entity's cost to implement and maintain security measures to protect against a breach of security relative to its resources.

"Reasonable security measures" would mean security measures that are reasonable for a covered entity to implement and maintain, including consideration of all of the following:

-- Designation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security (an owner or manager may designate himself or herself for purposes of this subdivision).
-- Identification of internal and external risks of a breach of security.
-- Adoption of appropriate information safeguards that are designed to address identified risks of a breach of security and assess the effectiveness of those safeguards.
-- Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information.
-- Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information.

Breach of Security Investigation

If a covered entity determined that a breach of security had or could have occurred, it would have to conduct a good-faith and prompt investigation that included all of the following:

-- An assessment of the nature and scope of the breach.
-- Identification of any sensitive personally identifying information that was involved in the breach and the identity of any State residents to whom that information related.
-- A determination of whether the information had been acquired or was reasonably believed to have been acquired by an unauthorized person.
-- Identification and implementation of measures to restore the security and confidentiality of the systems, if any, compromised in the breach.

In determining whether sensitive personally identifying information had been acquired by an unauthorized person without valid authorization, the following factors could be considered:

-- Indications that the information was in the physical possession and control of an unauthorized person.
-- Indications that the information had been downloaded or copied by an unauthorized person.
-- Indications that the information was used in an unlawful manner by an unauthorized person.
-- Whether the information was publicly displayed.

Notice of Breach

If a covered entity that owned or licensed sensitive personally identifiable information determined that a breach had occurred, it would have to provide notice of the breach to each State resident whose information was acquired in the breach. A covered entity would have to provide notice to State residents as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the entity to conduct an investigation and determine the scope of the breach. Except as otherwise provided, the entity would have to provide notice within 45 days of its determination that a breach had occurred.

If a Federal or State law enforcement agency determined that notice to State residents would interfere with a criminal investigation or national security, and delivered a request to the covered entity for a delay, the entity would have to delay providing the notice for a period that the agency determined was necessary. If the law enforcement agency determined that an additional delay was necessary, it would have to deliver a written request to the covered entity for an additional delay, and the covered entity would have to extend the delay as provided in written request.

Except as otherwise provided, a covered entity would have to provide notice to a State resident in compliance with one of the following, as applicable:

-- In the case of a breach that involved a username or password, in combination with any password or security question and answer that would permit access to an online account, and no other information was involved, the entity could provide the notice in electronic or other form that directed the affected resident to promptly change his or her password and security question or answer, as applicable, or to take other appropriate steps to protect the online account with the covered entity and all other accounts for which the resident whose information had been breached used the same username or e-mail address and password or security question or answer.
-- In the case of a breach that involved information for login credentials of an e-mail account furnished by the covered entity, it could not comply by providing the notification to that e-mail address, but could comply, instead, by providing notice by another method described in the bill, or by providing clear and conspicuous notice delivered to the State resident online if he or she were connected to the account from an internet protocol address or online location from which the entity knew the resident customarily accessed the account.
-- Except as otherwise provided, the entity would have to provide written notice sent to the resident's mailing address in the records of the covered entity, or by e-mail notice sent to the e-mail address of the State resident in the records of the covered entity.

Under the third scenario, the notice would have to include, at least, all of the following: 1) the date, estimated date, or estimated date range of the breach, 2) a description of the information acquired by an unauthorized person as part of the breach, 3) a general description of the actions taken by the covered entity to restore the security and confidentiality of the information involved in the breach, 4) a general description of steps a State resident could take to protect himself or herself from identity theft, if the breach created a risk of identity theft, and 5) contact information that the resident could use to contact the entity to inquire about the breach.

Substitute Notice

A covered entity that was required to provide notice to a State resident could provide substitute notice instead of direct notice, if direct notice were not feasible because of any of the following:

-- Lack of sufficient contact information for the State resident who the covered entity was required to notify.
-- Excessive cost to the covered entity of providing direct notification relative to its resources.

For the purposes of the above provision, the cost of direct notification to State residents would be considered excessive if it exceeded $250,000.

Substitute notice would have to include both of the following:

-- If the covered entity maintained a website, a conspicuous notice posted on the website for at least 30 days.
-- Notice in print and in broadcast media, including major media in urban and rural areas where the State residents who the covered entity was required to notify reside.

If a covered entity determined that notice was not required, the entity would have to document the determination in writing and maintain records concerning the determination for at least five years.

Written Notice to the DTMB

If the number of State residents who a covered entity was required to notify exceeded 750, it would have to provide written notice of the breach to the DTMB as expeditiously as possible and without unreasonable delay. Except as otherwise provided, the entity would have to provide the notice within 45 days of its determination that a breach had occurred.

The notice would have to include all of the following:

-- A synopsis of the events surrounding the breach at the time that notice was provided.
-- The approximate number of State residents the entity was required to notify.
-- Any services related to the breach the entity was offering or was scheduled to offer without charge to residents, and instructions on how to use them.
-- How a resident could obtain additional information about the breach from the entity.

A covered entity could provide the Department with supplemental or updated information regarding a breach at any time.

Information marked as confidential that was obtained by the Department would not subject to the Freedom of Information Act.

Notifying Consumer Reporting Agencies

If a covered entity discovered circumstances that required that it provide notice to more than 1,000 State residents at a single time, it also would have to notify, without unreasonable delay, each consumer reporting agency that compiled and maintained files on consumers on a nationwide basis as defined under Federal law, of the timing, distribution, and content of the notices.

Third-Party Agent

If a third-party agent experienced a breach of security in the system it maintained, the agent would have to notify the covered entity of the breach of security as quickly as practicable. After receiving notice from a third-party agent, a covered entity would have to provide notices required under the Act. A third-party agent, in cooperation with a covered entity, would have to provide information in its possession so that the entity could comply with its notice requirements.

A covered entity could enter into a contractual agreement with a third-party agent under which the agent agreed to handle notifications required under the Act.

Penalties

A person that knowingly violated or had violated a notification requirement could be ordered

to pay a civil fine of not more than $2,000 for each violation, or not more than $5,000 per day for each consecutive day that the covered entity failed to take reasonable action to comply with the Act's notice requirements. A person's aggregate liability for civil fines for multiple violations related to the same security breach could not exceed $250,000. The Attorney General would have exclusive authority to bring an action to recover a civil fine.

It would not be a violation of the Act to refrain from providing any notice required under the bill if a court of competent jurisdiction had directed otherwise.

To the extent that notification was required as the result of a breach experienced by a third-party agent, a failure to inform the covered entity of the breach would be a violation by the third-party agent and it would be subject to the remedies and penalties described above.

The remedies would be independent and cumulative. The availability of a remedy would not affect any right or cause of action a person could have at common law, by statute, or otherwise.

The proposed Act would not provide a basis for a private right of action.

State Agency Responsibilities

State agencies would be subject to the Act's notice requirements. A State agency that acquired and maintained sensitive personally identifying information from a State government employer, and that was required to provide notice to any State resident, also would have to notify the employing State agency of any State residents to whom the information related.

A claim or civil action for a violation of the bill by a State agency would be subject to the governmental immunity Law.

By February 1 of each year, the DTMB would have to submit a report to the Governor, the Senate Majority Leader, and the Speaker of the House of Representatives that described the nature of any reported breaches of security by State agencies or third-party agents of State agencies in the preceding calendar year along with recommendations for security improvements. The report would have to identify any State agency that had violated any of the applicable requirements in the bill in the preceding calendar year.

Disposal of Data

A covered entity or third-party agent would have to take reasonable measures to dispose, or arrange for the disposal, of records that contained sensitive personally identifying information within its custody or control when retention of the records was no longer required under applicable law, regulations, or business needs. Disposal would have to include shredding, erasing, or otherwise modifying the information in the records to make it unreadable or undecipherable through any reasonable means consistent with industry standards.

Exempt Entities

An entity that was subject to or regulated under Federal laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the Federal government would be exempt from the bill as long as the entity did all of the following:

-- Maintained procedures under those laws, rules, regulations, procedures, or guidance.
-- Provided notice to consumers under those laws, rules, regulations, procedures, or guidance.

-- Timely provided a copy of the notice to the DTMB when the number of State residents the entity notified exceeded 750.

Except as otherwise provided, an entity that was subject to or regulated under State laws, rules, regulations, procedures, or guidance on data breach notification that were established or enforced by State government, and were at least as thorough as the notice requirements provided by bill, would be exempt from the bill so long as the entity did all of the following:

-- Maintained procedures under those laws, rules, regulations, procedures, or guidance.
-- Provided notice to customers under the notice requirements of those laws, rules, regulations, procedures, or guidance.
-- Timely provided a copy of the notice to the DTMB when the number of state residents the entity notified exceeded 750.

An entity that was subject to or regulated under the Insurance Code would be exempt from the bill.

An entity that owned, was owned by, or was under common ownership with an entity described above and that maintained the same cybersecurity procedures as that other entity would be exempt from the bill.

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

FISCAL IMPACT

The bills would have a cost to 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 that would require 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 6405 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.

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

SAS\S1718\s6405sa

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.