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

BILL ANALYSIS

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

House Bill 4186 (Substitute H-2 as passed by the House)
House Bill 4187 (Substitute H-7 as passed by the House)
Sponsor: Representative Diana Farrington
House Committee: Financial Services
Way and Mean
Senate Committee: Regulatory Reform

Date Completed: 9-29-20

CONTENT

House Bill 4187 (H-7) would enact the "Data Breach Notification Act" to do the following:

- **Require business entities to implement and maintain reasonable security measures designed to protect sensitive personally identifying information against a breach of security.**
- **Require a covered entity to consider specified circumstances in developing its reasonable security measures.**
- **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 to provide notice of a breach to each Michigan resident whose sensitive personally identifiable information was acquired in the breach and require the notice to be sent within 45 days after the covered entity completed the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.**
- **Prescribe the information a notice would have to include, including the date or estimated date of the breach, a description of the sensitive personally identifying information that was acquired, and a general description of steps a resident could take to protect himself or herself from identity theft.**
- **Allow a covered entity to provide a substitute notice instead of a direct notice under certain circumstances.**
- **Require a third-party agent that experienced a breach of security to notify a covered entity of the breach.**
- **Subject State agencies to the notice requirements proposed in the Act.**
- **Require the Department of Technology, Management, and Budget (DTMB) to submit to the Governor, Senate Majority Leader, and Speaker of the House of Representatives by February 1 each year, a report describing any reported breaches of security by State agencies or third-party agents in the preceding calendar year.**
- **Prescribe penalties for violating the Act.**
- **Specify that certain entities would be exempt from the Act.**

House Bill 4186 (H-2) would amend the Identity Theft Protection Act to specify that Sections 12 and 12a of the Act would not apply to a covered entity, as that term is defined in the Data Breach Notification Act. (Section 12 prescribes certain notice

requirements regarding a security breach. Section 12a governs the destruction of data containing personal information.)

The bills are tie-barred. House Bill 4186 (H-2) would take effect on June 20, 2021.

House Bill 4187 (H-7) is described in greater detail below.

Definitions

The bill would define "breach of security" or "breach" as 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 occurs 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 is used for a purpose unrelated to the business of the covered entity or is subject to further unauthorized use.
-- A release of a public record that is 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.

"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 has more than 50 employees and owns or licenses sensitive personally identifying information, or a franchisee of any of the foregoing. The term also would include a State agency.

"Data in electronic form" would mean any data that is stored electronically on a computer system, database, or other technology, including recordable tapes and other mass storage devices. As used in this definition, "electronically" would mean a method using electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

"Sensitive personally identifying information" would mean a username or electronic mail (e-mail) address, in combination with a password, security question and answer, or similar information, 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. The term also 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 resident:

-- A nontruncated Social Security number.
-- A nontruncated driver license number, enhanced driver license number, State personal identification (ID) card number, enhanced State personal ID card number, passport number, military ID number, or other unique ID number issued on a government document that is used to verify the identity of a specific individual.
-- A financial account number, including, but not limited to, a bank account number, credit union account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, PIN, or similar security information, 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 ID number and any unique identifier used by a health insurer to identify the State resident.

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

-- Information about a State resident that has been lawfully made public by a Federal, State, or local government record or a widely distributed media.
-- Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify a State resident or that otherwise renders the information unusable, including encryption of the data or device containing the sensitive personally identifying information, unless the covered entity knows or reasonably believes that the encryption key or security credential that could render the personally identifying information readable or usable has been breached together with the information.

"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.

Reasonable Security Measures

The proposed Act would 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.

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 sensitive personally identifying information was accessed, acquired, or maintained by or on behalf of the covered entity.
-- The covered entity's cost to implement and maintain the 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:

-- Identification of internal and external risks of a breach of security.
-- Adoption of appropriate information safeguards that were designed to address identified risks of a breach of security and assess the effectiveness of those safeguards.
-- Retention of service providers, if any, that were 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.
-- 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 could designate himself or herself to coordinate the covered entity's security measures.

Breach of Security

Under the Act, if a covered entity determined that a breach of security had or could have occurred, the entity 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 sensitive personally identifying 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, such as a lost or stolen computer or other device containing information.
-- Indications that the information had been downloaded, copied, or otherwise acquired or transferred by an unauthorized person.
-- Indications that the information was used in an unlawful manner by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
-- Whether the information was publicly displayed.

Notice of Breach of Security

Under the Act, 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 sensitive personally identifiable information was acquired in the breach.

A covered entity would have to provide notice to those State residents as expeditiously as possible and without unreasonable delay. Except as otherwise provided, the covered entity would have to provide any required notice within 45 days after the covered entity completed the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database.

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 written or electronic request to the covered entity for a delay, a covered entity would have to delay providing the notice for a period that the law enforcement agency determined was necessary. If the law enforcement agency determined that an additional delay was necessary, it would have to deliver a written or electronic request to the covered entity for an additional delay, and the covered entity would have to delay providing the notice to the date specified in the law enforcement agency's request for additional delay, or extend the delay set forth in the original request for the additional period set forth in the request for additional delay.

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 of security 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 sensitive personally identifying information was involved, the covered entity could comply with this provision by providing the notification in electronic or other form that directed the State resident whose sensitive personally identifying information had been breached 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 State resident used the same username or e-mail address and password or security question or answer.
-- In the case of a breach that involved sensitive personally identifying information for login credentials of an e-mail account furnished by the covered entity, the covered entity could not comply with this provision by providing the notification to that e-mail address, but, instead, could comply with this provision by providing notice by another method described in this provision, or by providing clear and conspicuous notice delivered to the State resident online if the resident were connected to the online account from an internet protocol address or online location from which the covered entity knew the State resident customarily accessed the account.
-- Except as provided above, the covered entity would have to comply with this provision by providing a notice, in writing, sent to the mailing address of the State resident 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.

The notice would have to include, at a minimum, all of the following:

-- The date, estimated date, or estimated date range of the breach.
-- A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.
-- A general description of the actions taken by the covered entity to restore the security and confidentiality of the personal information involved in the breach.
-- 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.
-- Contact information that the State resident could use to contact the covered entity to inquire about the breach.

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

The cost of direct notification to State residents would be considered excessive if it exceeded $250,000 or if notice would have to be provided to more than 500,000 State residents.

Substitute notice would have to include both of the following:

-- If the covered entity maintained an internet website, a conspicuous notice posted on the website for a period of 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 resided.

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.

If a covered entity discovered circumstances that required that it provide notice to more than 1,000 State residents at a single time, the entity 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 in 15 USC 1681a(p), of the timing, distribution, and content of the notices. (Under 15 USC 1681a(p), consumer reporting agency that compiles and maintains files on consumers on a nationwide basis means a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide: a) public record information and b) credit account information from people who furnish that information regularly and in the ordinary course of business.)

Third Party Breach of Security

Under the bill, if a third-party agent experienced a breach of security in the system maintained by the agent, it 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 the notice required under the bill. A third-party agent, in cooperation with a covered entity, would have to provide information in the possession of the third-party agent so that the covered entity could comply with its notice requirements.

A covered entity could enter into a contractual agreement with a third-party agent under which the third-party agent and covered entity agreed as to which party would be responsible for notifications to State residents required under the Act, and the cost thereof, when the third-party agent experienced a breach of security.

If a covered entity had not entered into a contractual agreement with a third-party agent and the third-party agent had not fulfilled its data security or privacy obligations under its customer or service agreement with the covered entity, the covered entity could seek reimbursement from the third-party agent, informally or through a civil action, for actual costs, including labor, associated with providing notices related to the breach of security experienced by the third-party agent.

State Agencies

Under the bill, State agencies would be subject to the notice requirements of the Act. 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 under the Act, 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 Act by a State agency would be subject to the Governmental Immunity Act.

DTMB Report

Under the bill, 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 Act in the preceding calendar year.

Record Disposal

The bill would require a covered entity or third-party agent 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 sensitive personally identifying information in the records to make it unreadable or undecipherable through any reasonable means consistent with industry standards.

Penalties

The bills specifies that a person who knowingly violated or had violated a notification requirement under the Act 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 notice requirements of the Act.

A person's aggregate liability for civil fines for multiple violations related to the same security breach could not exceed $750,000.

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 Act if a court of competent jurisdiction had directed otherwise.

To the extent that notification was required under the Act 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 of the Act by the third-party agent and the agent would be subject to the remedies and penalties described in the bill.

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 Act could not be construed to provide a basis for a private right of action.

Exemptions

Under the bill, 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 Act as long as it does both of the following:

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

An entity that was not subject to or regulated under Federal laws, rules, regulations, procedures, or guidance, but was subject to or regulated under state laws, rules, regulations,

procedures, or guidance on data breach notification that are established or enforced by state government, and were at least as thorough as the notice requirements provided by the Act, would be exempt from the Act as long as it did both of the following:

-- Maintained procedures under those state laws, rules, regulations, procedures, or guidance.
-- Provided notice to customers under the notice requirements of those state laws, rules, regulations, procedures, or guidance.

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

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 exempt from the Act.

Preemption

The bill states that the Act deals 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, directly or indirectly, any matter expressly set forth in the Act would be preempted.

MCL 445.64 (H.B. 4186) Legislative Analyst: Stephen Jackson

FISCAL IMPACT

House Bill 4186 (H-2)

The bill would have no fiscal impact on State or local government.

House Bill 4187 (H-7)

The bill would have an indeterminate fiscal impact on State government, local units of government, and nonpublic entities. The required notifications could have a fiscal impact on entities that do not have related procedures in place; however, the proposed requirements also could lead to cost savings if breaches were identified and addressed sooner. The amount of cost or savings is indeterminate and would depend on the actual number and size of the breaches of security.

The bill also provides for civil fines for violations of the proposed notification requirements. Revenue from civil fines is deposited into the State Justice System Fund. The Fund supports justice-related activities across State government in the Departments of Corrections, Health and Human Services, State Police, and Treasury. The Fund also supports justice-related issues in the Legislative Retirement System and the Judiciary.

Fiscal Analyst: Joe Carrasco
Elizabeth Raczkowski

SAS\S1920\s4186sa