Legislative Analysis

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

DATA BREACH NOTIFICATION ACT

Analysis available at
http://www.legislature.mi.gov

House Bills 4186 and 4187 as introduced
Sponsor: Rep. Diana Farrington
Committee: Financial Services
Complete to 2-20-19

BRIEF SUMMARY:

House Bill 4187 would create a new act, the "Data Breach Notification Act." The act would require certain entities to do all of the following:

- Protect sensitive personal identifying information.
- Investigate actual and potential breaches of security.
- Provide notice to persons in the event of a breach of security resulting in unauthorized acquisition of sensitive personal identifying information.

The act would also specify certain powers and duties of governmental officers and entities and provide for penalties and remedies.

House Bill 4186 would amend the Identify Theft Protection Act (MCL 445.64) to exempt covered entities, as defined in and regulated by the Data Breach Identification Act, from sections 12 and 12a of the Identify Theft Protection Act, which pertain to security breaches and notifications.

House Bills 4186 and 4187 are tie-barred to each other, meaning that neither could take effect unless the other were also enacted.

Both bills would take effect January 20, 2020.

DETAILED SUMMARY:

House Bill 4187 would create the Data Breach Notification Act, and House Bill 4186 would exempt entities subject to the new act from similar provisions of the Identity Theft Protection Act. The proposed new act is described in greater detail below.

Definitions
As used in the Data Breach Notification Act:

"Breach of security" or "breach" would mean the unauthorized acquisition of sensitive personally identifying information in electronic form if the acquisition were reasonably likely to cause substantial risk of identity theft or fraud to individuals to whom the information related. Acquisition occurring over a period of time committed by the same entity would be considered one breach. The term would exclude the following:

- A good-faith acquisition of sensitive personally identify 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 this state or a political subdivision of this state.

"Covered entity" would mean an individual or a sole proprietorship, partnership, government entity (including a state agency), 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.
"Data in electronic form" would mean any data stored electronically or digitally on any computer system or other database, including recordable tapes and other mass storage devices.

"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 him or her:

- A nontruncated Social Security number, driver license number, state personal identification card number, passport number, military identification number, or other unique identification number issued on a government document.
- A financial account number.
- A medical or mental history, treatment, or diagnosis issued by a health care professional.
- A health insurance policy number or subscriber identification number and any unique identifier used by a health insurer.
- A username or email address, in combination with a password or a security question and answer, that would allow access to an online account that is likely to have or is used to obtain sensitive personally identifying information.

Sensitive personally identifying information would <u>exclude</u> information about a state resident that has been lawfully made public by a federal, state, or local government record or a widely distributed media or information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify a resident or otherwise renders the information unusable—unless it is known that the encryption key or security credential has been breached along with the 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.

<u>Reasonable security measures</u>
Under the new act, 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 need to consider all of the following in developing its security measures:

- The size of the covered entity.
- The amount of sensitive personally identifying information owned or licensed by the covered entity and the type of activities for which the information is accessed, acquired, or maintained by or on its behalf.
- 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:

- Designation of an employee or employees to coordinate security measures to protect against a breach of security.
- Identification of internal and external risks of a breach of security.
- Adoption of appropriate information safeguards designed to address identified risks and assess the effectiveness of those safeguards.
- Retention of service providers contractually required to maintain appropriate safeguards for sensitive personally identifying information.
- Evaluation and adjustment of security measures to account for changes in circumstance affecting the security of sensitive personally identifying information.

Breach of security

If a covered entity determines that a breach of security has or may have occurred, it would have to conduct a good-faith and prompt investigation including all of the following:

- Assessing the nature and scope of the breach.
- Identifying any sensitive personally identifying information involved in the breach and any state residents to whom that information relates.
- Determining whether the information has been acquired or is reasonably believed to have been acquired by an unauthorized person.
- Identifying and implementing measures to restore the security and confidentiality of the systems, if any, compromised in the breach.

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

- Indications that the information is 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 has been downloaded or copied.
- Indications that the information was used in an unlawful manner, such as fraudulent accounts opened or instances of identity theft reported.
- Indications that the information was publicly displayed.

Notice of breach of security

If a covered entity that owns or licenses sensitive personally identifiable information determines that a breach occurred, it would have to provide notice of the breach to each state resident whose information was acquired in the breach as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation and determine the scope of the breach. The covered entity would need to provide notice within 45 days of its determination that a breach has occurred, unless a federal or state law enforcement agency determines that required notice to state residents would interfere with a criminal investigation or national security and delivers a request to the covered entity for a delay, in which case it would have to delay providing notice for a period the law enforcement agency determines is necessary, including additional delays.

A covered entity would have to provide notice to a state resident by delivering the notification in electronic or other form to the state resident in compliance with one of the following:

- For a breach that involves a username or password, in combination with any password or security question and answer permitting online access to an online account, and no other sensitive personally identifying information, by directing the state resident to promptly change his or her password and security question or answer, or other similar appropriate steps.
- For a breach that involves sensitive personally identifying information for login credentials of an email account, the covered entity would not be complying with notification requirements by sending the notice to that email address. Notice could be delivered to the resident online if the resident were connected to the online account from an internet protocol address or online location from which the covered entity knows the state resident customarily accesses the account.
- Except as provided above, the covered entity would have to comply by sending a written notice to the mailing address of the resident or by email notice. The notice would have to include at least all of the following:
  - The date, estimated date, or estimated date range of the breach.
  - A description of the sensitive personally identifying information acquired as part of the breach.
  - A general description of the actions taken to restore the security and confidentiality of the personal information involved in the breach.
  - A general description of steps a state resident can take to protect against identity theft, if the breach creates a risk of identity theft.
  - Contact information that the state resident can use to ask about the breach.

Substitute notice

A covered entity required to provide notice could instead provide substitute notice, if direct notice is not feasible because of any of the following:

- Excessive cost to the covered entity of providing direct notification relative to the resources of the covered entity. For example, the cost of direct notification would be considered excessive if it exceeded $250,000.
- Lack of sufficient contact information for the state resident to be notified.

Substitute notice would require a conspicuous notice to be posted on the covered entity's website, if any, for a period of at least 30 days, and notice in print and in broadcast media, including major media in urban and rural areas where the state residents to be notified reside. If a covered entity determines notice not to be required, it would need to document that determination in writing and maintain records concerning the determination for at least five years.

Notice to the Department of Technology, Management, and Budget

If the number of state residents to be notified exceeds 750, the entity would have to provide written notice of the breach to the Department of Technology, Management, and Budget (DTMB) as expeditiously as possible and without unreasonable delay. The covered entity would have to provide the notice within 45 days after its determination that a breach had occurred. Written notice to the DTMB would have to include all of the following:

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

A covered entity could provide the DTMB with supplemental or updated information regarding a breach at any time. Information marked as confidential obtained by the DTMB would not be subject to the Freedom of Information Act (FOIA).

Notification of consumer reporting agencies

A covered entity that is required to provide notice to more than 1,000 state residents at a single time would also have to notify, without unreasonable delay, each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis of the timing, distribution, and content of the notices.

Notice of system breach by third party

If a third-party agent experienced a breach of security in the system maintained by the agent, the agent would be required to notify the covered entity of the breach as quickly as practicable. After receiving notice from a third-party agent, a covered entity would need to provide the required notices described above. 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 also enter into a contractual agreement with a third-party agent in which the third-party agent agrees to handle required notifications.

Violation of notification requirements

A person that knowingly violates a notification requirement could be ordered to pay a civil fine of up to $2,000 for each violation or not more than $5,000 per day for each consecutive day the covered entity fails to take reasonable action to comply with the requirements. A person's aggregate liability for civil 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.

Sensitive records disposal

A covered entity or third-party agent would have to take reasonable measures to dispose or arrange for the disposal of records that contain sensitive personally identifying information when retention of the records is 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 making it unreadable or undecipherable through any reasonable means consistent with industry standards.

Exemptions

An entity 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 the entity maintained procedures and provided notice under those laws, rules, regulations, procedures, or guidance. The entity would also have to timely provide a copy of the notice to the DTMB when the number of state residents the entity notified exceeds 750.

An entity 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 are at least as thorough as the requirements under the act, would be exempt from the act as long as the entity maintained procedures and provided notice to customers under those laws, rules, regulations, procedures, or guidance. The entity would also have to timely provide a copy of the notice to the DTMB when the number of state residents the entity notified exceeds 750.

An entity subject to or regulated under the Insurance Code would be exempt from the act.

An entity that owns, is owned by, or is common ownership with an exempt entity described above and that maintains the same cybersecurity procedures as that exempt entity would also be exempt from the act.

Annual report

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 describing 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. The report would have to identify any state agency that violated any applicable requirements in the preceding calendar year.

FISCAL IMPACT:

House Bill 4187 would have an indeterminate fiscal impact on state government, local units of government, and nonpublic entities that own or license personally identifying information. Public and private entities would incur costs in implementing and maintaining

reasonable security measures and notifying affected residents as described in the bill if such measures and procedures are not already in place. However, protection measures, as well as early identification and containment of breaches, have also been shown to reduce the costs of breaches.

The Department of Technology, Management, and Budget would likely incur one-time and ongoing IT costs to develop a means to receive, organize, and maintain breach notifications. As of August 2018, the median IT project cost in the state is $111,000. Ongoing costs for system maintenance and data storage would likely exceed $10,000.

The state government currently investigates security breaches of state information and is required to notify affected residents of the breach "without unreasonable delay" under the Identity Theft Protection Act. The bill would require a notice to be provided within 45 days of identifying a breach. The bill could result in cost savings to the state if it leads to security breaches being identified and contained within a shorter time. The most recent annual study on the cost of data breaches by the Ponemon Institute reports that costs of security breaches are significantly lower the sooner they are either identified or contained. [1]

The bill could affect costs for certain nonpublic entities depending on the entities' current information security policies and whether the bill's requirements lead to earlier detection and containment. Entities may incur costs from the requirement to directly notify residents of a security breach. The study by the Ponemon Institute states that notification costs in the United States are exceptionally high at an average of $740,000 per breach. The bill would permit entities to notify residents by an alternate means if the cost of direct notification exceeded $250,000.

The bill could increase revenues to the state, depending on the number of persons violating notification requirements and the number of days that notification requirements are not complied with. Revenue collected from payment of civil fines is deposited into the state Justice System Fund, which supports various justice-related endeavors in the judicial and legislative branches of government and the Departments of State Police, Corrections, Health and Human Services, and Treasury.

House Bill 4186 would have no direct fiscal impact on the state or local units of government.

Legislative Analyst: E. Best
Fiscal Analyst: Michael Cnossen

■ This analysis was prepared by nonpartisan House Fiscal Agency staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.

[1] 2018 Cost of a Data Breach Study: Global Overview. Ponemon Institute LLC. July 2018.