192523-1 : n : 03/01/2018 : CMH / th LSA2018-20517

ORR FLOOR SUBSTITUTE FOR SB318

SYNOPSIS: This bill would create the Data Breach Notification Act to require certain entities to provide notice to certain persons upon a breach of security that results in the unauthorized acquisition of sensitive personally identifying information.

A BILL

TO BE ENTITLED

AN ACT

Relating to consumer protection; to require certain entities to provide notice to certain persons upon a breach of security that results in the unauthorized acquisition of sensitive personally identifying information.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. This act may be cited and shall be known as the Alabama Data Breach Notification Act of 2018.

Section 2. For the purposes of this act, the following terms have the following meanings:

(1) BREACH OF SECURITY or BREACH. The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach. The term does 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 or subject to further unauthorized use.

b. The release of a public record not otherwise subject to confidentiality or nondisclosure requirements.

c. Any lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state.

(2) COVERED ENTITY. A person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information.

(3) DATA IN ELECTRONIC FORM. Any data stored electronically or digitally on any computer system or other database, including, but not limited to, recordable tapes and other mass storage devices.

(4) GOVERNMENT ENTITY. Any division, bureau, commission, regional agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing sensitive personally identifying information.

(5) INDIVIDUAL. Any Alabama resident whose sensitive personally identifying information was, or the covered entity reasonably believes to have been, accessed as a result of the breach.

(6) SENSITIVE PERSONALLY IDENTIFYING INFORMATION.

a. Except as provided in paragraph b., an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident:

1. A non-truncated Social Security number or tax identification number.

2. A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.

3. 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 credit or debit the financial account.

4. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

6. A user name or email 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.

b. The term does not include either of the following:

1. Information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media.

2. Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.

(7) THIRD-PARTY AGENT. An entity that has been contracted to maintain, store, process, or is otherwise permitted to access sensitive personally identifying

information in connection with providing services to a covered entity.

Section 3. (a) Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security.

(b) Reasonable security measures means security measures practicable for the covered entity to implement and maintain, including consideration of all of the following:

(1) 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.

(2) Identification of internal and external risks of a breach of security.

(3) Adoption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards.

(4) Retention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information.

(5) Evaluation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information.

(6) Keeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measures.

(c) An assessment of a covered entity's security shall be based upon the entity's security measures as a whole and shall place an emphasis on data security failures that are multiple or systemic, including consideration of all the following:

(1) The size of the covered entity.

(2) The amount of sensitive personally identifying information and the type of activities for which the sensitive personally identifying information is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity.

(3) The covered entity's cost to implement and maintain the security measures to protect against a breach of security relative to its resources.

Section 4. (a) If a covered entity determines that a breach of security has or may have occurred in relation to sensitive personally identifying information that is accessed, acquired, maintained, stored, utilized, or communicated by, or on behalf of, the covered entity, the covered entity shall conduct a good faith and prompt investigation that includes all of the following:

(1) An assessment of the nature and scope of the breach.

(2) Identification of any sensitive personally identifying information that may have been involved in the breach and the identity of any individuals to whom that information relates.

(3) A determination of whether the sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

(4) Identification and implementation of measures to restore the security and confidentiality of the systems compromised in the breach.

(b) In determining whether sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person without valid authorization, the following factors may be considered:

(1) Indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information.

(2) Indications that the information has been downloaded or copied.

(3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(4) Whether the information has been made public.

Section 5. (a) A covered entity that is not a third-party agent that determines under Section 4 that, as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably

believed to have been acquired by an unauthorized person, and is reasonably likely to cause substantial harm to the individuals to whom the information relates, shall give notice of the breach to each individual.

(b) Notice to individuals under subsection (a) shall be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation in accordance with Section 4. Except as provided in subsection (c), the covered entity shall provide notice within 45 days of the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

(c) If a federal or state law enforcement agency determines that notice to individuals required under this section would interfere with a criminal investigation or national security, the notice shall be delayed upon the written request of the law enforcement agency for a period that the law enforcement agency determines is necessary. A law enforcement agency, by a subsequent written request, may revoke the delay as of a specified date or extend the period set forth in the original request made under this section if further delay is necessary.

(d) Except as provided by subsection (e), notice to an affected individual under this section shall be given in writing, sent to the mailing address of the individual in the records of the covered entity, or by email notice sent to the

email address of the individual in the records of the covered entity. The notice shall include, at a minimum, all of the following:

(1) The date, estimated date, or estimated date range of the breach.

(2) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.

(3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach.

(4) A general description of steps a consumer can take to protect himself or herself from identity theft.

(5) Information that the individual can use to contact the covered entity to inquire about the breach.

(e)(1) A covered entity required to provide notice to any individual under this section may provide substitute notice in lieu of direct notice, if direct notice is not feasible due to any of the following:

a. Excessive cost to the covered entity required to provide such notification relative to the resources of the covered entity, provided that the cost of the individual notification is considered excessive if it exceeds five hundred thousand dollars ($500,000).

b. Lack of sufficient contact information for the individual required to be notified.

c. The affected individuals exceed 100,000 persons.

(2) Substitute notice shall include both of the following:

a. A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website, for a period of 30 days.

b. Notice in print and in broadcast media, including major media in urban and rural areas where the affected individuals reside.

c. An alternative form of substitute notice may be used with the approval of the Attorney General.

(f) If a covered entity determines that notice is not required under this section, the entity shall document the determination in writing and maintain records concerning the determination for no less than five years.

Section 6. (a) If the number of individuals a covered entity is required to notify under Section 5 exceeds 1,000, the entity shall provide written notice of the breach to the Attorney General as expeditiously as possible and without unreasonable delay. Except as provided in subsection (c) of Section 5, the covered entity shall provide the notice within 45 days of the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.

(b) Written notice to the Attorney General shall include all of the following:

(1) A synopsis of the events surrounding the breach at the time that notice is provided.

(2) The approximate number of individuals in the state who were affected by the breach.

(3) Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use the services.

(4) The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

(c) A covered entity may provide the Attorney General with supplemental or updated information regarding a breach at any time.

(d) Information marked as confidential that is obtained by the Attorney General under this section is not subject to any open records, freedom of information, or other public record disclosure law.

Section 7. If a covered entity discovers circumstances requiring notice under Section 5 of more than 1,000 individuals at a single time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. 1681(a)(p), of the timing, distribution, and content of the notices.

Section 8. In the event a third-party agent has experienced a breach of security in the system maintained by the agent, the agent shall notify the covered entity of the breach of security as expeditiously as possible and without unreasonable delay, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. After receiving notice from a third-party agent, a covered entity shall provide notices required under Sections 5 and 6. A third-party agent, in cooperation with a covered entity, shall provide information in the possession of the third-party agent so that the covered entity can comply with its notice requirements. A covered entity may enter into a contractual agreement with a third-party agent whereby the third-party agent agrees to handle notifications required under this act.

Section 9. (a) A violation of the notification provisions of this act is an unlawful trade practice under the Alabama Deceptive Trade Practices Act, Chapter 19, Title 8, Code of Alabama 1975, but does not constitute a criminal offense under Section 8-19-12, Code of Alabama 1975. The Attorney General shall have the exclusive authority to bring an action for civil penalties under this act.

(1) A violation of this act does not establish a private cause of action under Section 8-19-10, Code of Alabama 1975. Nothing in this act may otherwise be construed to affect any right a person may have at common law, by statute, or otherwise.

(2) Any covered entity or third-party agent who is knowingly engaging in or has knowingly engaged in a violation of the notification provisions of this act will be subject to the penalty provisions set out in Section 8-19-11, Code of Alabama 1975. For the purposes of this act, knowingly shall mean willfully or with reckless disregard in failing to comply with the notice requirements of Sections 5 and 6. Civil penalties assessed under Section 8-19-11, Code of Alabama 1975, shall not exceed five hundred thousand dollars ($500,000) per breach.

(b)(1) Notwithstanding any remedy available under subdivision (2) of subsection (a) of this section, a covered entity that violates the notification provisions of this act shall be liable for a civil penalty of not more than five thousand dollars ($5,000) per day for each consecutive day that the covered entity fails to take reasonable action to comply with the notice provisions of this act.

(2) The office of the Attorney General shall have the exclusive authority to bring an action for damages in a representative capacity on behalf of any named individual or individuals. In such an action brought by the office of the Attorney General, recovery shall be limited to actual damages suffered by the person or persons, plus reasonable attorney's fees and costs.

(3) It is not a violation of this act to refrain from providing any notice required under this act if a court of competent jurisdiction has directed otherwise.

(4) To the extent that notification is required under this act as the result of a breach experienced by a third-party agent, a failure to inform the covered entity of the breach shall subject the third-party agent to the fines and penalties set forth in the act.

(5) Government entities shall be subject to the notice requirements of this act. A government entity that acquires and maintains sensitive personally identifying information from a government employer, and which is required to provide notice to any individual under this act, must also notify the employing government entity of any individual to whom the information relates.

(6) A violation of this act by a government entity is governed by Section 36-1-12, Code of Alabama 1975, and Article I, Section 14 of the Constitution of Alabama of 1901, now appearing as Section 14 of the Official Recompilation of the Constitution of Alabama of 1901, as amended.

(7) By February 1 of each year, the Attorney General shall submit a report to the Governor, the President Pro Tempore of the Senate, and the Speaker of the House of Representatives describing the nature of any reported breaches of security by government entities or third-party agents of government entities in the preceding calendar year along with recommendations for security improvements. The report shall identify any government entity that has violated any of the applicable requirements in this act in the preceding calendar year.

Section 10. A covered entity or third-party agent shall take reasonable measures to dispose, or arrange for the disposal, of records containing sensitive personally identifying information within its custody or control when the records are no longer to be retained pursuant to applicable law, regulations, or business needs. Disposal shall include shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any reasonable means consistent with industry standards.

Section 11. An entity subject to or regulated by federal laws, rules, regulations, procedures, or guidance on data breach notification established or enforced by the federal government is exempt from this act as long as the entity does all of the following:

(1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance.

(2) Provides notice to consumers pursuant to those laws, rules, regulations, procedures, or guidance.

(3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.

Section 12. An entity subject to or regulated by 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 notice

requirements provided by this act, is exempt from this act so long as the entity does all of the following:

(1) Maintains procedures pursuant to those laws, rules, regulations, procedures, or guidance.

(2) Provides notice to customers pursuant to the notice requirements of those laws, rules, regulations, procedures, or guidance.

(3) Timely provides a copy of the notice to the Attorney General when the number of individuals the entity notified exceeds 1,000.

Section 13. This act shall become effective on the first day of the third month following its passage and approval by the Governor, or its otherwise becoming law.