SB238

173854-2

By Senator Orr

RFD: Fiscal Responsibility and Economic Development

First Read: 16-FEB-16

173854-2:n:02/11/2016:JET/tj LRS2016-564R1

SYNOPSIS: Existing law does not require a person that owns, licenses, or maintains data containing personal information of an Alabama resident to notify the resident if the personal information is breached by an unauthorized person.

This bill would create the Alabama Information Protection Act of 2016 to provide for the protection of sensitive personally identifying information and notice to individuals whose personal information has been breached.

This bill would require specified entities, including governmental entities and third-party agents, to notify the Attorney General and the individual owners of personal information upon a data security breach.

This bill would require these entities to provide notice to credit reporting agencies of security breaches of personal information involving more than 1,000 individuals.

This bill would require the Attorney General to annually report certain information relating to security breaches to the Governor and the Legislature.

This bill would provide for the disposal of records containing sensitive personally identifying personal information, would authorize enforcement actions by the Attorney General, and would provide for the assessment of civil penalties for failure to provide the required notification.

A BILL

TO BE ENTITLED

AN ACT

Relating to consumer protection; to require specified entities to take generally acceptable industry practices and measures to protect and secure data containing sensitive personally identifying information in paper or electronic form; to require the entities to notify the Attorney General of data security breaches; to require notice to individuals and credit reporting agencies of data security breaches in certain circumstances; to provide for the disposal of customer records; to provide for enforcement actions by the Attorney General; to provide civil penalties; to provide that this act does not create a private cause of action; and to provide certain exemptions.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. This act may be cited and shall be known as the Alabama Information Protection Act of 2016.

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

(1) ACCESS DEVICE. A card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, or debit card.

(2) BREACH OF SECURITY or BREACH. The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Good faith acquisition of sensitive personally identifying information by an employee or agent of the covered entity does not constitute a breach of security unless the information is used for a purpose unrelated to the business or subject to further unauthorized use. Acquisition occurring over a period of time committed by the same entity constitutes one single breach.

(3) COVERED ENTITY. A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other business entity that acquires, maintains, stores, or uses sensitive personally identifying information. For purposes of the notice requirements of Sections 4 through 7, the term includes a governmental entity.

(4) CUSTOMER RECORDS. Any material on which personal information is recorded or preserved by any means, including, but not limited to, written or spoken words, graphically

depicted, printed, or electromagnetically transmitted that are provided by a resident of this state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

(5) DATA IN ELECTRONIC FORM. Any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

(6) FINANCIAL INSTITUTION. A bank, trust company with banking powers, savings bank, industrial loan company, savings association, credit union, or other lender regulated by a state or federal agency.

(7) GOVERNMENTAL 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.

(8) MICROPROCESSOR CHIP DATA. The data contained in the microprocessor chip of an access device.

(9) MAGNETIC STRIP DATA. The data contained in the magnetic stripe of an access device.

(10) PIN. A personal identification code that identifies the cardholder.

(11) PIN VERIFICATION CODE NUMBER. The data used to verify cardholder identity when a PIN is used in a transaction.

(12) SENSITIVE PERSONALLY IDENTIFYING INFORMATION. Includes an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

a. A Social Security number.

b. A driver's license or state-issued identification card number.

c. A financial account number or credit or debit card number, in combination with any required security code, PIN, access code, or password that is necessary to permit access to a financial account.

The term does not include any of the following:

a. Information about an individual which has been lawfully made public by federal, state, or local governmental entity records or a widely distributed media.

b. Information that is 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 encryption key has also been breached.

c. Information that includes no more than the last four digits of an individual's Social Security number.

d. Information that includes credit or debit card account information that is appropriately masked with no more

than the last four and first six digits of the account number showing.

(13) THIRD-PARTY AGENT. An entity that has been contracted to maintain, store, or process sensitive personally identifying information on behalf of a covered entity or governmental entity.

Section 3. Each covered entity and governmental entity shall take reasonable security measures to protect and secure data in electronic form containing sensitive personally identifying information.

Section 4. (a) A covered entity shall provide notice described in subsection (b) to the Attorney General of any verified breach of security affecting 1,000 or more residents of this state. The notice must be provided to the Attorney General as expeditiously as practicable, but no later than 60 days after the determination of the breach. A covered entity may receive an additional 15 days to provide notice as required in this section if good cause for delay is provided in writing to the Attorney General within 60 days after determination of the breach. This notification is subject to the law enforcement determinations specified in subsection (b) of Section 5.

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

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

(2) The number of individuals in this 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 residents, and instructions as to how to use such 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 information regarding a breach at any time.

(d) Confidential information obtained by the Attorney General pursuant to this section must be maintained under seal, and is not subject to any open records, freedom of information, or other public record disclosure law.

Section 5. (a) Except as provided in subsections (b) and (c), in the event there is a breach of security affecting 1,000 or more individuals in this state, a covered entity shall give notice to each resident in this state whose sensitive personally identifying information the covered entity determines was acquired as a result of the breach. Notice to individuals must be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the

reasonable integrity of the data system that was breached, but no later than 60 days after the determination of the breach unless subject to a delay authorized under subsection (b) or waiver under subsection (c).

(b) If a federal or state law enforcement agency determines that notice to individuals required under this subsection 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 subsection if further delay is necessary.

(c) Notwithstanding subsection (a), notice to the affected residents is not required if, after an appropriate investigation, the covered entity reasonably determines that the breach has not and will not substantially result in financial harm to the individuals whose sensitive personally identifying information has been acquired. Such a determination must be documented in writing and maintained in its files.

(d) Notice to an affected resident under this section shall be by one of the following methods:

(1) Written notice sent to the mailing address of the resident in the records of the covered entity.

(2) Email notice sent to the email address of the resident in the records of the covered entity.

(e) The notice to an individual with respect to a breach of security shall include, at a minimum, all of the following:

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

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

(3) Information that the resident can use to contact the covered entity to inquire about the breach of security.

(f) A covered entity required to provide notice to any resident under this section may provide substitute notice in lieu of direct notice if the direct notice is not feasible because the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), because the affected individuals exceed 500,000 persons, or because the covered entity does not have an email address or mailing address for 200 of the affected individuals. The substitute notice shall include both of the following:

(1) A conspicuous notice on the Internet website of the covered entity, if the covered entity maintains a website.

(2) Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

(g)(1) Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to comply with the notice requirement of this section if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator in the event of a breach of security.

(2) A covered entity that timely provides a copy of notice authorized by this subsection to the Attorney General is deemed to comply with the notice requirement of Section 4.

Section 6. If a covered entity discovers circumstances requiring notice under Section 5 of more than 1,000 residents of this state at a single time, the covered 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. § 1681a(p), of the timing, distribution, and content of the notices.

Section 7. 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 practicable, but no later than 10 days after the agent determines that a breach occurred.

Section 8. By February 1 of each year, the Attorney General shall submit a report to the Governor, the President of the Senate, and the Speaker of the House of Representatives describing the nature of any reported breaches of security by governmental entities or third-party agents of governmental entities in the preceding calendar year along with recommendations for security improvements. The report shall identify any governmental entity that has violated any of the applicable requirements in this act in the preceding calendar year.

Section 9. A covered entity shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal 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 means.

Section 10. (a)(1) Except as provided in subdivision (2), a violation of this act is a deceptive trade practice under Chapter 19, Title 8, Code of Alabama 1975, and does not constitute a criminal offense.

(2) A violation of this act does not establish a private cause of action under Section 8-19-10, Code of Alabama 1975.

(3) The act does not otherwise establish a private cause of action, but in no way affects any statutory or common law right that otherwise exists.

(b)(1) In addition to any remedy available under subsection (a), a covered entity that violates Section 4 or Section 5 is liable for a civil penalty not to exceed fifty thousand dollars ($50,000).

(2) The civil penalties for failure to notify provided in this subsection shall apply per breach and not per individual affected by the breach.

(c) All penalties collected pursuant to this subsection shall be deposited into the State Treasury to the credit of the General Fund, except that portion which represents the reasonable costs incurred by the Attorney General to recover the penalties, which shall be deposited to the credit of the operating fund of the Attorney General.

(d) 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.

(e) To the extent that the breach is a result of the acts or omissions of a third-party agent of the covered entity, the fines and penalties set forth in this act shall be levied on the third-party agent.

Section 11. (a) This act does not apply to a financial institution, or insurer as defined in subsection (2) of Section 27-1-2, Code of Alabama 1975, that is subject to the privacy and security provisions of the Gramm-Leach-Bliley

Act, Pub. L. No. 106-102, or similar rules as provided by the Alabama Department of Insurance.

(b) This act does not apply to a financial institution that is subject to the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended.

(c) This act does not apply to a provider of health care, a health care service plan, a health insurer, a covered entity, or business associate governed by the medical privacy and security rules issued by the United States Department of Health and Human Services, Parts 160 and 164, Title 45, Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

(d) A governmental entity is not liable for any damages resulting from a violation of this act, subject to Section 36-1-12, Code of Alabama 1975.

Section 12. 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.