SB106

163391-6

By Senator Orr

RFD: Judiciary

First Read: 03-MAR-15

163391-6:n:02/27/2015:JET/mfc LRS2014-3376R3

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 2015 to provide for the protection of personal 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 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.

This bill would also prohibit a person from retaining certain data from a credit, debit, or other financial card for a specified period of time and would require persons in violation to reimburse financial institutions for certain costs upon a breach of security.

A BILL

TO BE ENTITLED

AN ACT

Relating to consumer protection; to require specified entities to take reasonable measures to protect and secure data containing personal 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; to prohibit a person from retaining certain data from a charge, debit, or other financial card for a specified period of time; to provide certain exemptions; to require persons in violation to reimburse financial institutions of certain costs upon a breach of security; and to provide exceptions.

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 2015.

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, debit card, or stored value card.

(2) BREACH OF SECURITY or BREACH. The unauthorized access, loss, disclosure, or destruction of data in paper or electronic form containing personal information. Good faith access of personal 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.

(3) CARD SECURITY CODE. A value printed on an access device or contained in the microprocessor chip or magnetic stripe of an access device which is used to validate access device information during the authorization process.

(4) COVERED ENTITY. A sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other business entity that acquires, maintains, stores, or uses personal information. The term includes a third-party agent of a covered entity and, for purposes of the notice requirements of Sections 4 through 7, a governmental entity.

(5) CUSTOMER RECORDS. Any material, regardless of the physical form, 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 an individual in this state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

(6) 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.

(7) 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.

(8) 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 personal information.

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

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

(11) PERSONAL INFORMATION. Includes either of the following:

a. 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:

1. A Social Security number.

2. A driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity.

3. A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's 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.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include any of the following:

a. Information about an individual which has been made publicly available by a federal, state, or local governmental entity.

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.

c. Information that includes only the last four digits of an individual's Social Security number.

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

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

(14) SERVICE PROVIDER. A person or entity that stores, processes, or transmits access device data on behalf of another person.

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

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

Section 4. (a) A covered entity shall provide notice to the Attorney General of any breach of security affecting 500 or more individuals in this state. The notice must be provided to the Attorney General as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe that a breach occurred. 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 30 days after determination of the breach or reason to believe that a breach occurred.

(b) Written notice to the Attorney General under subsection (a) 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 or potentially have been 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 as to how to use such services.

(4) A copy of the notice required under this section or an explanation of the other actions taken pursuant to this section.

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

(c)(1) A covered entity must provide all of the following information to the Attorney General upon his or her request:

a. A police report, incident report, or computer forensics report.

b. A copy of the policies in place regarding breaches.

c. Steps that have been taken to rectify the breach.

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

Section 5. (a) Except as provided in subsections (b) and (c), a covered entity shall give notice to each individual in this state whose personal information the covered entity reasonably believes to have been accessed 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 30 days after the covered entity has reason to believe that a breach occurred 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, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably 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 to a specified date if further delay is necessary.

(c) Notwithstanding subsection (a), notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least five years. The covered entity shall provide the written determination to the Attorney General within 30 days after the determination.

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

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

(2) E-mail notice sent to the e-mail address of the individual 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 personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security.

(3) Information that the individual can use to contact the covered entity to inquire about the breach of security and the personal information that the covered entity maintained about the individual.

(f) A covered entity required to provide notice to an individual 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 e-mail 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 individuals 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. 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) A violation of this act is a deceptive trade practice under Chapter 19, Title 8, Code of Alabama 1975.

(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 five hundred thousand dollars ($500,000), as follows:

a. In the amount of one thousand dollars ($1,000) for each day up to 30 days after any violation of Section 4 or Section 5 and, thereafter, fifty thousand dollars ($50,000) for each subsequent 30-day period or portion thereof for up to 180 days.

b. If notice is not made within 180 days, in an amount not to exceed five hundred thousand dollars ($500,000).

(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) Except as provided in Section 11, this act does not establish a private cause of action.

Section 11. (a)(1) A person conducting business in this state that accepts an access device in connection with a transaction may not retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction, or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

(2) A person is in violation of this subsection if its service provider retains such data subsequent to the

authorization of the transaction, or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

(b)(1) If there is a breach of the security of the system of a person that has violated subsection (a), or a breach of the security of the system of that person's service provider, that person shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any of the following costs:

a. The cancellation or reissuance of any access device affected by the breach.

b. The closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts.

c. The opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach.

d. Any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach.

e. The notification of cardholders affected by the breach.

(2) The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person that has violated subsection (a). Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subsection are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

Section 12. (a) Except for subsection (b) of Section 11, this act does not apply to a financial institution that is subject to and in compliance with the privacy and security provisions of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102.

(b) A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, 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, is deemed to be in compliance with this act.

(c) A provider of health care, a health care service plan, a health insurer, or a covered entity 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) is deemed to be in compliance with this act.

(d) A governmental entity is not liable for any damages resulting from a violation of this act.

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.