

1 HB291
2 173854-2
3 By Representative Rowe
4 RFD: Military and Veterans Affairs
5 First Read: 24-FEB-16

2
3
4
5
6
7
8 SYNOPSIS: Existing law does not require a person that
9 owns, licenses, or maintains data containing
10 personal information of an Alabama resident to
11 notify the resident if the personal information is
12 breached by an unauthorized person.

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

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

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

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

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

11
12 A BILL
13 TO BE ENTITLED
14 AN ACT

15
16 Relating to consumer protection; to require
17 specified entities to take generally acceptable industry
18 practices and measures to protect and secure data containing
19 sensitive personally identifying information in paper or
20 electronic form; to require the entities to notify the
21 Attorney General of data security breaches; to require notice
22 to individuals and credit reporting agencies of data security
23 breaches in certain circumstances; to provide for the disposal
24 of customer records; to provide for enforcement actions by the
25 Attorney General; to provide civil penalties; to provide that
26 this act does not create a private cause of action; and to
27 provide certain exemptions.

1 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

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

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

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

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

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

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

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

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

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

13 (7) GOVERNMENTAL ENTITY. Any division, bureau,
14 commission, regional agency, board, district, authority,
15 agency, or other instrumentality of this state that acquires,
16 maintains, stores, or uses data in electronic form containing
17 sensitive personally identifying information.

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

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

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

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

1 (12) SENSITIVE PERSONALLY IDENTIFYING INFORMATION.

2 Includes an individual's first name or first initial and last
3 name in combination with any one or more of the following data
4 elements for that individual:

5 a. A Social Security number.

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

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

12 The term does not include any of the following:

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

16 b. Information that is encrypted, secured, or
17 modified by any other method or technology that removes
18 elements that personally identify an individual or that
19 otherwise renders the information unusable, including
20 encryption of the data, document, or device containing the
21 sensitive personally identifying information, unless the
22 encryption key has also been breached.

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

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

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

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

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

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

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

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

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

3 (3) Any services related to the breach being offered
4 or scheduled to be offered, without charge, by the covered
5 entity to residents, and instructions as to how to use such
6 services.

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

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

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

17 Section 5. (a) Except as provided in subsections (b)
18 and (c), in the event there is a breach of security affecting
19 1,000 or more individuals in this state, a covered entity
20 shall give notice to each resident in this state whose
21 sensitive personally identifying information the covered
22 entity determines was acquired as a result of the breach.
23 Notice to individuals must be made as expeditiously as
24 practicable and without unreasonable delay, taking into
25 account the time necessary to allow the covered entity to
26 determine the scope of the breach of security, to identify
27 individuals affected by the breach, and to restore the

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

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

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

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

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

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

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

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

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

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

13 (f) A covered entity required to provide notice to
14 any resident under this section may provide substitute notice
15 in lieu of direct notice if the direct notice is not feasible
16 because the cost of providing notice would exceed two hundred
17 fifty thousand dollars (\$250,000), because the affected
18 individuals exceed 500,000 persons, or because the covered
19 entity does not have an email address or mailing address for
20 200 of the affected individuals. The substitute notice shall
21 include both of the following:

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

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

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

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

13 Section 6. If a covered entity discovers
14 circumstances requiring notice under Section 5 of more than
15 1,000 residents of this state at a single time, the covered
16 entity shall also notify, without unreasonable delay, all
17 consumer reporting agencies that compile and maintain files on
18 consumers on a nationwide basis, as defined in the Fair Credit
19 Reporting Act, 15 U.S.C. § 1681a(p), of the timing,
20 distribution, and content of the notices.

21 Section 7. In the event a third-party agent has
22 experienced a breach of security in the system maintained by
23 the agent, the agent shall notify the covered entity of the
24 breach of security as expeditiously as practicable, but no
25 later than 10 days after the agent determines that a breach
26 occurred.

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

11 Section 9. A covered entity shall take all
12 reasonable measures to dispose, or arrange for the disposal,
13 of customer records containing personal information within its
14 custody or control when the records are no longer to be
15 retained pursuant to applicable law, regulations, or business
16 needs. Disposal shall include shredding, erasing, or otherwise
17 modifying the personal information in the records to make it
18 unreadable or undecipherable through any means.

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

23 (2) A violation of this act does not establish a
24 private cause of action under Section 8-19-10, Code of Alabama
25 1975.

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

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

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

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

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

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

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

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

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

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

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

20 Section 12. This act shall become effective on the
21 first day of the third month following its passage and
22 approval by the Governor, or its otherwise becoming law.