

1 SB318
2 191614-1
3 By Senators Orr and Holley
4 RFD: Governmental Affairs
5 First Read: 13-FEB-18

2
3
4
5
6
7
8 SYNOPSIS: This bill would create the Data Breach
9 Notification Act to require certain entities to
10 provide notice to certain persons upon a breach of
11 security that results in the unauthorized
12 acquisition of sensitive personally identifying
13 information.

14
15 A BILL
16 TO BE ENTITLED
17 AN ACT

18
19 Relating to consumer protection; to require certain
20 entities to provide notice to certain persons upon a breach of
21 security that results in the unauthorized acquisition of
22 sensitive personally identifying information.

23 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

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

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

1 (1) BREACH OF SECURITY or BREACH. The unauthorized
2 acquisition of data in electronic form containing sensitive
3 personally identifying information. Acquisition occurring over
4 a period of time committed by the same entity constitutes one
5 breach. The term does not include any of the following:

6 a. Good faith acquisition of sensitive personally
7 identifying information by an employee or agent of a covered
8 entity, unless the information is used for a purpose unrelated
9 to the business or subject to further unauthorized use.

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

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

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

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

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

1 (5) INDIVIDUAL. Any Alabama resident whose personal
2 information was, or the covered entity reasonably believes to
3 have been, accessed as a result of the breach.

4 (6) SENSITIVE PERSONALLY IDENTIFYING INFORMATION.

5 a. Except as provided in paragraph b., an
6 individual's first name or first initial and last name in
7 combination with one or more of the following:

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

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

15 3. A financial account number, including a bank
16 account number, credit card number, or debit card number, in
17 combination with any security code, access code, password,
18 expiration date, or PIN, that is necessary to access the
19 financial account or to conduct a transaction that will credit
20 or debit the financial account.

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

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

1 6. A user name or email address, in combination with
2 a password or security question and answer that would permit
3 access to an online account affiliated with the covered entity
4 that is reasonably likely to contain or is used to obtain
5 sensitive personally identifying information.

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

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

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

21 (7) THIRD-PARTY AGENT. An entity that has been
22 contracted to maintain, store, process, or is otherwise
23 permitted to access sensitive personally identifying
24 information in connection with providing services to a covered
25 entity.

26 Section 3. (a) Each covered entity and third-party
27 agent shall implement and maintain reasonable security

1 measures to protect sensitive personally identifying
2 information against a breach of security.

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

6 (1) Designation of an employee or employees to
7 coordinate the covered entity's security measures to protect
8 against a breach of security. An owner or manager may
9 designate himself or herself.

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

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

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

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

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

24 (c) An assessment of a covered entity's security
25 shall be based upon the entity's security measures as a whole
26 and shall place an emphasis on data security failures that are

1 multiple or systemic, including consideration of all the
2 following:

3 (1) The size of the covered entity.

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

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

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

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

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

25 (3) A determination of whether the sensitive
26 personally identifying information has been acquired or is
27 reasonably believed to have been acquired by an unauthorized

1 person, and is reasonably likely to cause substantial harm to
2 the individuals to whom the information relates.

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

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

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

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

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

20 (4) Whether the information has been made public.

21 Section 5. (a) A covered entity that is not a
22 third-party agent that determines under Section 4 that, as a
23 result of a breach of security, sensitive personally
24 identifying information has been acquired or is reasonably
25 believed to have been acquired by an unauthorized person, and
26 is reasonably likely to cause substantial harm to the

1 individuals to whom the information relates, shall give notice
2 of the breach to each individual.

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

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

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

1 entity. The notice shall include, at a minimum, all of the
2 following:

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

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

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

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

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

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

19 a. Excessive cost to the covered entity required to
20 provide such notification relative to the resources of the
21 covered entity.

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

24 c. The affected individuals exceed 500,000 persons.

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

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

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

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

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

13 Section 6. (a) If the number of individuals a
14 covered entity is required to notify under Section 5 exceeds
15 1,000, the entity shall provide written notice of the breach
16 to the Attorney General as expeditiously as possible and
17 without unreasonable delay. Except as provided in subsection
18 (c) of Section 5, the covered entity shall provide the notice
19 within 45 days of the covered entity's determination that a
20 breach has occurred and is reasonably likely to cause
21 substantial harm to the individuals to whom the information
22 relates.

23 (b) Written notice to the Attorney General shall
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 approximate number of individuals in the
2 state who were 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 individuals, and instructions on how to use the
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) Information marked as confidential that is
14 obtained by the Attorney General under this section is not
15 subject to any open records, freedom of information, or other
16 public record disclosure law.

17 Section 7. If a covered entity discovers
18 circumstances requiring notice under Section 5 of more than
19 1,000 individuals at a single time, the entity shall also
20 notify, without unreasonable delay, all consumer reporting
21 agencies that compile and maintain files on consumers on a
22 nationwide basis, as defined in the Fair Credit Reporting Act,
23 15 U.S.C. 1681(a)(p), of the timing, distribution, and content
24 of the notices.

25 Section 8. In the event a third-party agent has
26 experienced a breach of security in the system maintained by
27 the agent, the agent shall notify the covered entity of the

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

13 Section 9. (a) A violation of this act is an
14 unlawful trade practice under the Alabama Deceptive Trade
15 Practices Act, Chapter 19, Title 8, Code of Alabama 1975, but
16 does not constitute a criminal offense under Section 8-19-12,
17 Code of Alabama 1975.

18 (1) A violation of this act does not establish a
19 private cause of action under Section 8-19-10, Code of Alabama
20 1975. Nothing in this act may otherwise be construed to affect
21 any right a person may have at common law, by statute, or
22 otherwise.

23 (2) Any covered entity or third-party agent who is
24 knowingly engaging in or has knowingly engaged in a violation
25 of this act will be subject to the penalty provisions set out
26 in Section 8-19-11, Code of Alabama 1975. For the purposes of
27 this act, knowingly shall mean willfully or with reckless

1 disregard in failing to comply with the notice requirements of
2 Sections 5 and 6. Civil penalties assessed under Section
3 8-19-11, Code of Alabama 1975, shall not exceed five hundred
4 thousand dollars (\$500,000) per breach.

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

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

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

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

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

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

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

23 Section 10. A covered entity or third-party agent
24 shall take reasonable measures to dispose, or arrange for the
25 disposal, of records containing sensitive personally
26 identifying information within its custody or control when the
27 records are no longer to be retained pursuant to applicable

1 law, regulations, or business needs. Disposal shall include
2 shredding, erasing, or otherwise modifying the personal
3 information in the records to make it unreadable or
4 undecipherable through any means.

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

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

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

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

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