

1 SB318
2 192523-5
3 By Senators Orr and Holley
4 RFD: Governmental Affairs
5 First Read: 13-FEB-18

1 SB318

2
3
4 ENROLLED, An Act,

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

9 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

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

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

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

19 a. Good faith acquisition of sensitive personally
20 identifying information by an employee or agent of a covered
21 entity, unless the information is used for a purpose unrelated
22 to the business or subject to further unauthorized use.

23 b. The release of a public record not otherwise
24 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. The State, a county, or a municipality or any instrumentality of the state, a county, or a municipality.

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

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

14 (7) THIRD-PARTY AGENT. An entity that has been
15 contracted to maintain, store, process, or is otherwise
16 permitted to access sensitive personally identifying
17 information in connection with providing services to a covered
18 entity.

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

23 (b) Reasonable security measures means security
24 measures practicable for the covered entity subject to

subsection (c), 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; provided, however, that the management of a government entity subject to this subdivision may be appropriately informed of the status of its security measures through a properly convened execution session under the Open Meetings Act pursuant to Section 36-25A-7, Code of Alabama 1975.

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

6 (1) The size of the covered entity.

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

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

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

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

24 (2) Identification of any sensitive personally
25 identifying information that may have been involved in the

1 breach and the identity of any individuals to whom that
2 information relates.

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

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

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

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

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

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

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

1 Section 5. (a) A covered entity that is not a
2 third-party agent that determines under Section 4 that, as a
3 result of a breach of security, sensitive personally
4 identifying information has been acquired or is reasonably
5 believed to have been acquired by an unauthorized person, and
6 is reasonably likely to cause substantial harm to the
7 individuals to whom the information relates, shall give notice
8 of the breach to each individual.

9 (b) Notice to individuals under subsection (a) shall
10 be made as expeditiously as possible and without unreasonable
11 delay, taking into account the time necessary to allow the
12 covered entity to conduct an investigation in accordance with
13 Section 4. Except as provided in subsection (c), the covered
14 entity shall provide notice within 45 days of the covered
15 entity's receipt of notice from a third party agent that a
16 breach has occurred or upon the covered entity's determination
17 that a breach has occurred and is reasonably likely to cause
18 substantial harm to the individuals to whom the information
19 relates.

20 (c) If a federal or state law enforcement agency
21 determines that notice to individuals required under this
22 section would interfere with a criminal investigation or
23 national security, the notice shall be delayed upon the
24 receipt of written request of the law enforcement agency for a
25 period that the law enforcement agency determines is

1 necessary. A law enforcement agency, by a subsequent written
2 request, may revoke the delay as of a specified date or extend
3 the period set forth in the original request made under this
4 section if further delay is necessary.

5 (d) Except as provided by subsection (e), notice to
6 an affected individual under this section shall be given in
7 writing, sent to the mailing address of the individual in the
8 records of the covered entity, or by email notice sent to the
9 email address of the individual in the records of the covered
10 entity. The notice shall include, at a minimum, all of the
11 following:

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

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

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

20 (4) A general description of steps an affected
21 individual can take to protect himself or herself from
22 identity theft.

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

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

5 a. Excessive cost. The term includes either of the
6 following:

7 1. Excessive cost to the covered entity relative to
8 the resources of the covered entity.

9 2. The cost to the covered entity exceeds five
10 hundred thousand dollars (\$500,000).

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

13 c. The affected individuals exceed 100,000 persons.

14 (2) a. Substitute notice shall include both of the
15 following:

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

19 2. Notice in print and in broadcast media, including
20 major media in urban and rural areas where the affected
21 individuals reside.

22 b. An alternative form of substitute notice may be
23 used with the approval of the Attorney General.

24 (f) If a covered entity determines that notice is
25 not required under this section, the entity shall document the

1 determination in writing and maintain records concerning the
2 determination for no less than five years.

3 Section 6. (a) If the number of individuals a
4 covered entity is required to notify under Section 5 exceeds
5 1,000, the entity shall provide written notice of the breach
6 to the Attorney General as expeditiously as possible and
7 without unreasonable delay. Except as provided in subsection
8 (c) of Section 5, the covered entity shall provide the notice
9 within 45 days of the covered entity's receipt of notice from
10 a third party agent that a breach has occurred or upon the
11 entity's determination that a breach has occurred and is
12 reasonably likely to cause substantial harm to the individuals
13 to whom the information relates.

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

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

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

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

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

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

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

11 Section 7. If a covered entity discovers
12 circumstances requiring notice under Section 5 of more than
13 1,000 individuals at a single time, the entity shall also
14 notify, without unreasonable delay, all consumer reporting
15 agencies that compile and maintain files on consumers on a
16 nationwide basis, as defined in the Fair Credit Reporting Act,
17 15 U.S.C. 1681a, of the timing, distribution, and content of
18 the notices.

19 Section 8. In the event a third-party agent has
20 experienced a breach of security in the system maintained by
21 the agent, the agent shall notify the covered entity of the
22 breach of security as expeditiously as possible and without
23 unreasonable delay, but no later than 10 days following the
24 determination of the breach of security or reason to believe
25 the breach occurred. After receiving notice from a third-party

1 agent, a covered entity shall provide notices required under
2 Sections 5 and 6. A third-party agent, in cooperation with a
3 covered entity, shall provide information in the possession of
4 the third-party agent so that the covered entity can comply
5 with its notice requirements. A covered entity may enter into
6 a contractual agreement with a third-party agent whereby the
7 third-party agent agrees to handle notifications required
8 under this act.

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

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

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

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

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

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

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

23 (4) To the extent that notification is required
24 under this act as the result of a breach experienced by a
25 third-party agent, a failure to inform the covered entity of

1 the breach shall subject the third-party agent to the fines
2 and penalties set forth in the act.

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

10 (6) All government entities are exempt from any
11 civil penalty authorized by this act; provided, however, the
12 Attorney General may bring an action against any state,
13 county, or municipal official or employee, in his or her
14 official capacity, who is subject to this act for any of the
15 following:

16 a. To compel the performance of his or her duties
17 under this act.

18 b. To compel the performance of his or her
19 ministerial acts under this act.

20 c. To enjoin him or her from acting in bad faith,
21 fraudulently, beyond his or her authority, or under mistaken
22 interpretation of the law.

23 (7) By February 1 of each year, the Attorney General
24 shall submit a report to the Governor, the President Pro
25 Tempore of the Senate, and the Speaker of the House of

1 Representatives describing the nature of any reported breaches
2 of security by government entities or third-party agents of
3 government entities in the preceding calendar year along with
4 recommendations for security improvements. The report shall
5 identify any government entity that has violated any of the
6 applicable requirements in this act in the preceding calendar
7 year.

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

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

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

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

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

6 Section 12. An entity subject to or regulated by
7 state laws, rules, regulations, procedures, or guidance on
8 data breach notification that are established or enforced by
9 state government, and are at least as thorough as the notice
10 requirements provided by this act, is exempt from this act so
11 long as the entity does all of the following:

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

14 (2) Provides notice to affected individuals pursuant
15 to the notice requirements of those laws, rules, regulations,
16 procedures, or guidance.

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

20 Section 13. 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.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

President and Presiding Officer of the Senate

Speaker of the House of Representatives

SB318

Senate 01-MAR-18

I hereby certify that the within Act originated in and passed
the Senate, as amended.

Patrick Harris,
Secretary.

House of Representatives
Amended and passed 22-MAR-18

Senate concurred in House amendment 27-MAR-18

By: Senator Orr