

2
3 SENATE GOVERNMENTAL AFFAIRS COMMITTEE SUBSTITUTE FOR SB318
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 sensitive
2 personally identifying information was, or the covered entity
3 reasonably believes to have been, accessed as a result of the
4 breach.

5 (6) SENSITIVE PERSONALLY IDENTIFYING INFORMATION.

6 a. Except as provided in paragraph b., an Alabama
7 resident's first name or first initial and last name in
8 combination with one or more of the following with respect to
9 the same Alabama resident:

10 1. A non-truncated Social Security number or tax
11 identification number.

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

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

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

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

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

9 b. The term does not include either of the
10 following:

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

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

24 (7) THIRD-PARTY AGENT. An entity that has been
25 contracted to maintain, store, process, or is otherwise
26 permitted to access sensitive personally identifying

1 information in connection with providing services to a covered
2 entity.

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

7 (b) Reasonable security measures means security
8 measures practicable for the covered entity to implement and
9 maintain, including consideration of all of the following:

10 (1) Designation of an employee or employees to
11 coordinate the covered entity's security measures to protect
12 against a breach of security. An owner or manager may
13 designate himself or herself.

14 (2) Identification of internal and external risks of
15 a breach of security.

16 (3) Adoption of appropriate information safeguards
17 to address identified risks of a breach of security and assess
18 the effectiveness of such safeguards.

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

22 (5) Evaluation and adjustment of security measures
23 to account for changes in circumstances affecting the security
24 of sensitive personally identifying information.

25 (6) Keeping the management of the covered entity,
26 including its board of directors, if any, appropriately
27 informed of the overall status of its security measures.

1 (c) An assessment of a covered entity's security
2 shall be based upon the entity's security measures as a whole
3 and shall place an emphasis on data security failures that are
4 multiple or systemic, including consideration of all the
5 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 security measures to protect against a breach of
14 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
26 breach and the identity of any individuals to whom that
27 information relates.

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

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

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

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

18 (2) Indications that the information has been
19 downloaded or copied.

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

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

24 Section 5. (a) A covered entity that is not a
25 third-party agent that determines under Section 4 that, as a
26 result of a breach of security, sensitive personally
27 identifying information has been acquired or is reasonably

1 believed to have been acquired by an unauthorized person, and
2 is reasonably likely to cause substantial harm to the
3 individuals to whom the information relates, shall give notice
4 of the breach to each individual.

5 (b) Notice to individuals under subsection (a) shall
6 be made as expeditiously as possible and without unreasonable
7 delay, taking into account the time necessary to allow the
8 covered entity to conduct an investigation in accordance with
9 Section 4. Except as provided in subsection (c), the covered
10 entity shall provide notice within 45 days of the covered
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 (c) If a federal or state law enforcement agency
15 determines that notice to individuals required under this
16 section would interfere with a criminal investigation or
17 national security, the notice shall be delayed upon the
18 written request of the law enforcement agency for a period
19 that the law enforcement agency determines is necessary. A law
20 enforcement agency, by a subsequent written request, may
21 revoke the delay as of a specified date or extend the period
22 set forth in the original request made under this section if
23 further delay is necessary.

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

1 email address of the individual in the records of the covered
2 entity. The notice shall include, at a minimum, all of the
3 following:

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

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

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

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

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

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

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

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

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

26 (2) Substitute notice shall include both of the
27 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 the notification
14 provisions of this act is an unlawful trade practice under the
15 Alabama Deceptive Trade Practices Act, Chapter 19, Title 8,
16 Code of Alabama 1975, but does not constitute a criminal
17 offense under Section 8-19-12, 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 the notification provisions of this act will be subject to
26 the penalty provisions set out in Section 8-19-11, Code of
27 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
26 the breach shall subject the third-party agent to the fines
27 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 reasonable means consistent with
5 industry standards.

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

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

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

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

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