

1 SB382
2 97195-2
3 By Senator Griffith
4 RFD: Governmental Affairs
5 First Read: 19-FEB-08

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

13 This bill would require a state agency or a
14 person that owns or licenses computerized data
15 containing the personal information of an Alabama
16 resident to notify the resident of a breach of
17 security involving the personal information.

18 This bill would require a state agency or
19 third-party person that maintains computerized data
20 containing personal information on behalf of
21 another agency or person to notify the agency or
22 person who owns or licenses the computerized data
23 of any breach of security.

24 This bill would provide limited exceptions
25 for the time and manner of the notification.

26 This bill would also provide standards for
27 storage and protection of computer data.

1 This bill would provide that the notice and
2 storage requirements do not apply to financial
3 institutions.

4 This bill would also provide that a person
5 who violates this act is liable to a financial
6 institution for the costs involved in protecting
7 its customers from a breach of security.

8
9 A BILL
10 TO BE ENTITLED
11 AN ACT

12
13 To provide a procedure for notification of a breach
14 of security where computer data containing the personal
15 information of an Alabama resident is disclosed to an
16 unauthorized person; to provide limited exceptions; to require
17 standards for the storage and protection of computer data
18 containing personal information; and to provide for limited
19 liability for breaches.

20 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

21 Section 1. For purposes of this act, the following
22 terms have the following meanings:

23 (1) ACCESS DEVICE. A card issued by a financial
24 institution that contains a magnetic stripe, microprocessor
25 chip, or other means for storage of information which
26 includes, but is not limited to, a credit card, debit card, or
27 stored value card.

1 (2) AGENCY. Any public agency of the executive
2 branch of the State of Alabama or its subdivisions.

3 (3) BREACH OF SECURITY. Unauthorized acquisition of
4 unencrypted and unredacted computerized data or encrypted
5 electronic data and the confidential process or key that
6 compromises the security, confidentiality, or integrity of the
7 personal information maintained by an individual or commercial
8 entity. Good faith acquisition of personal information by an
9 employee or agent of an individual or commercial entity for
10 the purposes of the individual or the commercial entity is not
11 a breach of the security system, provided that the personal
12 information is not used or disclosed by the person in an
13 unauthorized manner.

14 (4) PERSON. An individual, group of individuals,
15 partnership, association, corporation, or any other business
16 unit or legal entity. The term shall not include a financial
17 institution as defined in 15 U.S.C. § 6809.

18 (5)a. PERSONAL INFORMATION. An individual's first
19 name or first initial and last name in combination with any of
20 the following data elements, when the data elements, in whole
21 or in part, are not redacted:

22 1. Social Security number.

23 2. Account number, credit card number, or debit card
24 number, in combination with any required security code, access
25 code, or password that would permit access to an individual's
26 financial account.

1 b. Personal information does not include publicly
2 available information that is lawfully made available to the
3 general public from federal, state, or local government
4 records.

5 Section 2. (a) Any agency or person that conducts
6 business in Alabama and that possesses, acquires, maintains,
7 handles, collects, disseminates, owns, licenses, sells, or
8 otherwise deals with computerized data that contains the
9 personal information of an Alabama resident shall disclose any
10 breach of security of the data to any resident of Alabama
11 whose personal information is reasonably believed to have been
12 acquired by an unauthorized person. Except as provided in
13 subsection (c), following the determination of the breach, the
14 notification shall be given in the most expedient time and
15 manner possible and without unreasonable delay.

16 Notwithstanding the foregoing, the notification shall be
17 consistent with the legitimate needs of law enforcement, as
18 provided in subsection (d), and the agency or person may take
19 any measures necessary to determine the scope of the breach,
20 identify the individuals affected, and restore the reasonable
21 integrity of the system.

22 (b) An agency or a person that maintains on behalf
23 of another agency or person computerized data that contains
24 the personal information shall disclose to the agency or
25 person for whom that data is maintained any breach of security
26 of the data if the personal information is reasonably believed
27 to have been acquired by an unauthorized person. Following

1 determination of the breach, notification shall be given in
2 the most expedient time and manner possible and without
3 unreasonable delay. Notwithstanding the foregoing, the
4 notification shall be consistent with the legitimate needs of
5 law enforcement, as provided in subsection (d), and the agency
6 or person may take any measures necessary to determine the
7 scope of the breach, to identify the individuals affected, and
8 restore the reasonable integrity of the system.

9 (c) When a security breach occurs, an agency or
10 person subject to subsection (a) shall notify the owner of the
11 computer data containing personal information, in plain
12 language, of all of the following information if that
13 information is available at the time the notice is provided:

14 (1) The date of the notice.

15 (2) The name of the agency, person, or business that
16 maintained the computerized data at the time of the breach.

17 (3) The date or estimated date that the breach
18 occurred if possible to determine.

19 (4) A description of the categories of personal
20 information that is believed to have been, acquired by an
21 unauthorized person.

22 (d) The notification required by this section may be
23 delayed upon a request by law enforcement if a law enforcement
24 agency determines that the notification will impede a criminal
25 investigation. The notification time period required by
26 subsections (a) and (b) shall commence after the person
27 responsible for providing the notices receives notice from the

1 law enforcement agency that notification will not compromise
2 the investigation.

3 (e) Notice shall be provided by one of the following
4 methods:

5 (1) Written notice to the last known address of the
6 individual.

7 (2) Electronic notice sent to the most recent
8 electronic mail address of the individual in the records of
9 the business.

10 (3) Substitute notice, if the agency or person
11 responsible for providing notice demonstrates that the cost of
12 providing notice would exceed five hundred thousand dollars
13 (\$500,000) or that the affected class of persons subject to be
14 notified exceeds 200,000, the agency or person use may use a
15 substitute notice, which shall consist of all of the
16 following:

17 a. Email notice when the agency or person has an
18 email address for the subject persons.

19 b. Conspicuous posting of the notice on the web site
20 page of the agency or person, if the agency or person
21 maintains one.

22 c. Notification to statewide media.

23 (f) Notwithstanding the notification requirements in
24 subsection (e), if an agency or person responsible for
25 providing notice is required to provide notice pursuant to
26 federal law and that agency or person maintains notification
27 procedures pursuant to laws, rules, regulations, procedures,

1 or guidelines established by a federal regulating agency, the
2 agency or person shall be deemed to be in compliance with the
3 notification requirements of this section for any notification
4 made in accordance with the rules, regulations, procedures, or
5 guidelines established by the federal regulator.

6 (g) An agency or person required by subsection (a)
7 to notify more than 1,000 persons of a breach of security
8 pursuant to this act, shall also promptly notify all consumer
9 reporting agencies that compile and maintain files on
10 consumers on a nationwide basis, as defined by Section 603(p)
11 of the Fair Credit Reporting Act (15 U.S.C. § 1681a(p)), of
12 the timing, distribution, and content of the notices. Nothing
13 in this subsection shall be construed to require the agency or
14 person to provide the consumer reporting agency the names or
15 other personal identifying information of breach notice
16 recipients. An agency or person that is required to notify
17 consumer reporting agencies of a breach pursuant to Title V of
18 the Gramm-Leach-Bliley Act, approved November 12, 1999 (113
19 Stat. 14361 15 U.S.C. § 6801 et seq.) and that has provided
20 notification pursuant to that act shall be deemed to have
21 complied with this subsection.

22 (h) Upon receipt of notification of a breach
23 requiring notification of any resident of Alabama, a financial
24 institution or other licensee may communicate to the
25 individual owners of accounts affected of the nature, time,
26 and location where the breach occurred without civil or
27 criminal liability.

1 (i) Any person receiving notice required by this
2 section has a duty to take appropriate action to mitigate
3 damages, including, but not limited, to, placing a fraud alert
4 on his or her credit file.

5 Section 3. (a) Any agency that maintains personal
6 information or any person that conducts business in Alabama
7 shall destroy or arrange for the destruction of records
8 containing personal information within the person's or
9 agency's custody or control that are no longer necessary to be
10 retained by shredding, erasing, or otherwise modifying the
11 personal information in those records to make it unreadable or
12 undecipherable.

13 (b) No agency or person that accepts an access
14 device in connection with a transaction shall store, in either
15 encrypted or unencrypted form, subsequent to authorization,
16 the card security code data, the PIN verification code data,
17 the full contents of any track of a magnetic stripe or data
18 chip, card-validation code, or value, or any other security
19 information in a manner that permits access to an individual
20 financial account.

21 (c) Notwithstanding any other provision of law and
22 in addition to any other liability provided by law, if a
23 person violates subsection (a) or (b) of this section and such
24 violation results in a security breach, the person shall be
25 liable to a financial institution for reasonable costs of
26 actions taken by the financial institution to protect the
27 personal information and account information of the customer

1 or to continue to provide financial services to the customer,
2 including, but not limited to, any cost incurred as a result
3 of a potential or actual breach of data security in connection
4 with any of the following:

5 (1) Contacting any account holder affected by the
6 breach.

7 (2) The cancellation or reissuance of any credit,
8 debit, or other access device issued by any financial
9 institution.

10 (3) The closure of any deposit, transaction, or
11 other account and any action to stop payments or block
12 transactions with respect to the account.

13 (4) The opening or reopening of any deposit,
14 transaction, or other account for any customer of the
15 financial institution subsequent to action taken as a result
16 of the breach.

17 (5) Any refund or credit made to any customer of the
18 financial institution as a result of unauthorized
19 transactions.

20 Section 4. Any financial institution injured by a
21 violation of Section 2 or Section 3 of this act has a private
22 cause of action against a person responsible for the security
23 breach. A court shall award any of the following:

24 (1) The actual damages as described in Section 2.

25 (2) Incidental and consequential damages.

26 (3) Court costs and reasonable attorneys' fees.

1 Section 5. This act shall become effective on the
2 first day of the third month following its passage and
3 approval by the Governor, or its otherwise becoming law.