HB750

141554-1

By Representative Bridges

RFD: Technology and Research

First Read: 24-APR-12

141554-1:n:04/24/2012:DA/mfc LRS2012-1737

SYNOPSIS: Existing law does not require notification by certain data collectors upon a breach of security regarding personal information.

This bill would make such requirements.

A BILL

TO BE ENTITLED

AN ACT

To require notification by certain data collectors upon a breach of security regarding personal information.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. As used in this act, the following words shall have the following meanings:

(1) BREACH OF THE SECURITY SYSTEM. Unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of the individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an

information broker or data collector for the purposes of the information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(2) DATA COLLECTOR. Any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity. The term "data collector" shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

(3) INFORMATION BROKER. Any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, and shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

(4) NOTICE. Includes all of the following:

a. Written notice.

b. Telephone notice.

c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. §7001.

d. Substitute notice, if the information broker or data collector demonstrates that the cost of providing notice would exceed fifty thousand dollars ($50,000), that the affected class of individuals to be notified exceeds 100,000, or that the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following:

1. E-mail notice, if the information broker or data collector has an e-mail address for the individuals to be notified.

2. Conspicuous posting of the notice on the information broker's or data collector's website page, if the information broker or data collector maintains one.

3. Notification to major statewide media.

Notwithstanding any provision of this subdivision to the contrary, an information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.

(5) PERSON. Any individual, partnership, corporation, limited liability company, trust, estate,

cooperative association, or other entity. The term "person" as used in this act shall not be construed to require duplicative reporting by any individual, corporation, trust, estate, cooperative, association, or other entity involved in the same transaction.

(6) PERSONAL INFORMATION. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name of the data elements are not encrypted or redacted:

a. Social Security number.

b. Driver's license number or state identification card number.

c. Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords.

d. Account passwords or personal identification numbers or other access codes.

e. Any of the items contained in subparagraphs a. to d. when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Section 2. (a) Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breech in the security of the data to any resident of this state whose unencrypted personal information was acquired, or is reasonably believed to have been, by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c), or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(b) Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was acquired or is reasonably believed to have been, by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) In the event that an information broker or data collector discovers circumstances requiring notification pursuant to this section of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. §1681a. of the timing, distribution, and content of the notices.

(e) A violation of this section is deceptive trade practices pursuant to Chapter 19 of Title 8 of the Code of Alabama 1975.

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