By: Ellis

S.B. No. 223

A BILL TO BE ENTITLED

1 AN ACT

2 relating to a loss of computerized data or breach of computer

3 security involving sensitive personal information.

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

5 SECTION 1. The heading to Section 48.103, Business &

6 Commerce Code, as added by Chapter 294, Acts of the 79th

7 Legislature, Regular Session, 2005, is amended to read as follows:

8 Sec. 48.103. NOTIFICATION REQUIRED FOLLOWING BREACH OF

9 SECURITY OR LOSS OF CERTAIN COMPUTERIZED DATA.

10 SECTION 2. Section 48.103, Business & Commerce Code, as

11 added by Chapter 294, Acts of the 79th Legislature, Regular

12 Session, 2005, is amended by amending Subsections (b), (c), (d),

13 (g), and (h) and adding Subsection (i) to read as follows:

14 (b) A person that conducts business in this state, including

15 any state or local governmental entity in this state, that [and]

16 owns or licenses computerized data that includes sensitive personal

17 information shall disclose any breach of system security or loss of

18 the information, after discovering or receiving notification of the

19 breach or after discovering the loss, to any resident of this state

20 whose sensitive personal information was, or is reasonably believed

21 to have been, acquired by an unauthorized person or was lost. A

22 [The] disclosure required by this subsection shall be made as

23 quickly as possible, except as provided by Subsection (d) or as

24 necessary to determine the scope of the breach or loss and restore

1 the reasonable integrity of the <u>data or</u> data system.

2   (c) Any person<u>, including a state or local governmental</u>

3 <u>entity,</u> that maintains computerized data that includes sensitive

4 personal information that the person does not own shall notify the

5 owner or license holder of the information of any breach of system

6 security <u>or loss of the sensitive personal information</u> immediately

7 after discovering the breach <u>or loss</u>, if the sensitive personal

8 information was, or is reasonably believed to have been, acquired

9 by an unauthorized person <u>or was lost</u>.

10   (d) A person may delay providing notice as required by

11 Subsections (b)<u>,</u> [<s>and</s>] (c), <u>and (i)</u> at the request of a law

12 enforcement agency that determines that the notification will

13 impede a criminal investigation. The notification shall be made as

14 soon as the law enforcement agency determines that it will not

15 compromise the investigation.

16   (g) Notwithstanding Subsection (e), a person that maintains

17 its own notification procedures as part of an information security

18 policy for the treatment of sensitive personal information that

19 complies with the timing requirements for notice under this section

20 complies with <u>the notice requirements of</u> this section <u>other than</u>

21 <u>Subsection (i)</u> if the person notifies affected persons in

22 accordance with that policy.

23   (h) If a person is required by this section to notify at one

24 time more than 10,000 persons of a breach of system security <u>or loss</u>

25 <u>of sensitive personal information</u>, the person shall also notify,

26 without unreasonable delay, all consumer reporting agencies, as

27 defined by 15 U.S.C. Section 1681a, that maintain files on

1 consumers on a nationwide basis, of the timing, distribution, and

2 content of the notices.

3 (i) A person required to provide notice under Subsection (b)

4 or (c) shall, without unreasonable delay, also notify the attorney

5 general in writing of each incident involving a breach of system

6 security or loss of computerized data containing sensitive personal

7 information. The notice must contain:

8 (1) the person's name and address;

9 (2) the date the breach or loss was discovered;

10 (3) a summary of the circumstances surrounding the

11 breach or loss;

12 (4) the type of information that was lost, stolen, or

13 compromised;

14 (5) the number of persons whose sensitive personal

15 information was lost, stolen, or compromised as a result of the

16 incident; and

17 (6) the name, mailing address, and telephone number of

18 a contact person from whom a person affected by the incident may

19 request additional information.

20 SECTION 3. Subchapter B, Chapter 48, Business & Commerce

21 Code, as added by Chapter 294, Acts of the 79th Legislature, Regular

22 Session, 2005, is amended by adding Section 48.104 to read as

23 follows:

24 Sec. 48.104. REGISTRY OF PERSONS REPORTING BREACH OF

25 SECURITY OR LOSS OF CERTAIN COMPUTERIZED DATA. (a) The attorney

26 general shall establish and maintain a central registry of persons

27 required to provide notice under Section 48.103(b) or (c) of a

1 breach of system security or a loss of computerized data containing

2 sensitive personal information.

3 (b) The registry must include a record of each incident

4 involving a breach of system security or loss of sensitive personal

5 information reported under Section 48.103(i). The record must

6 contain the required information listed under that section.

7 (c) The registry may include other information the attorney

8 general considers necessary and appropriate to assist persons

9 receiving notice under Section 48.103 that their sensitive personal

10 information was lost, stolen, or compromised.

11 (d) The attorney general shall make the registry

12 information available to the public on request and by publishing it

13 on the attorney general's website. The attorney general shall

14 update the registry information on the website at least twice

15 monthly.

16 (e) Any sensitive personal information received by or in

17 connection with the operation of the registry by the attorney

18 general is confidential and not subject to disclosure under Chapter

19 552, Government Code.

20 (f) The attorney general may adopt rules necessary to

21 implement this section.

22 SECTION 4. The changes in law made by this Act apply only to

23 a breach of system security or loss of data containing sensitive

24 personal information that occurs on or after the effective date of

25 this Act. A breach of system security or loss of data containing

26 sensitive personal information that occurs before the effective

27 date of this Act is governed by the law in effect on the date the

1 breach or loss occurred, and the former law is continued in effect

2 for that purpose.

3   SECTION 5. Not later than January 1, 2008, the attorney

4 general shall establish the registry required by Section 48.104,

5 Business & Commerce Code, as added by this Act.

6   SECTION 6. This Act takes effect September 1, 2007.