

By: McCall, Rodriguez, Miller, Menendez,
Bohac

H.B. No. 1682

A BILL TO BE ENTITLED

AN ACT

relating to a breach in the security of a computerized data system that includes personal identifying information; providing a civil penalty.

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

SECTION 1. Title 4, Business & Commerce Code, is amended by adding Chapter 50 to read as follows:

CHAPTER 50. DISCLOSURES RELATING TO MAINTENANCE OF PERSONAL IDENTIFYING INFORMATION

Sec. 50.001. DEFINITIONS. In this chapter:

(1) "Consumer reporting agency" has the meaning assigned by Section 20.01.

(2) "Personal identifying information":

(A) means an individual's first name or first initial in combination with last name and with one or more of the following items of information:

(i) a social security number;

(ii) a driver's license number or other government-issued identification number; or

(iii) an account number or a credit or debit card number, in combination with any required security code, access code, or password that permits access to an individual's financial account; and

(B) does not include publicly available

1 information that is lawfully made available to the public from
2 federal, state, or local government records.

3 (3) "Service provider" means a person that is
4 authorized to hold or use a computerized database containing
5 personal identifying information on behalf of another person that
6 owns or licenses the database.

7 Sec. 50.002. BREACH OF SECURITY OF COMPUTERIZED DATA
8 SYSTEM. (a) For purposes of this chapter, a breach in the security
9 of a person's computerized data system is considered to have
10 occurred when there is unauthorized access to data electronically
11 stored in the system that compromises the security,
12 confidentiality, or integrity of personal identifying information
13 maintained by the person.

14 (b) Good faith access or acquisition of personal
15 identifying information by an employee or agent of the person is not
16 considered to be a breach in the security of the person's system for
17 purposes of this chapter if the personal identifying information is
18 not used or subject to further unauthorized disclosure.

19 Sec. 50.003. NOTIFICATION OF SECURITY BREACH. (a) A person
20 that owns or licenses computerized data that includes personal
21 identifying information of a resident of this state must notify the
22 resident of any breach of the security of the person's computerized
23 data system if the resident's unencrypted personal identifying
24 information was, or may have been, obtained by an unauthorized
25 person. Notification must be made promptly after the date the
26 person discovers the security breach, taking into consideration any
27 law enforcement agency requests as provided by Subsection (f) or

1 any measures necessary to determine the scope of the breach or
2 restore the reasonable integrity of the data system.

3 (b) A service provider holding or using computerized data
4 that includes unencrypted personal identifying information of a
5 resident of this state shall immediately notify and cooperate with
6 the owner or licensee of the information of any breach of the
7 security of the service provider's system if personal identifying
8 information was, or may have been, obtained by an unauthorized
9 person. In this subsection, the cooperation of a service provider
10 with the owner or licensee of the information includes sharing
11 information relevant to the breach.

12 (c) Except as provided by Subsection (d) or (e), the person
13 must provide the notification required by this section in writing
14 or by electronic notice, if the electronic notice complies with the
15 requirements regarding electronic records and signatures set forth
16 in 15 U.S.C. Section 7001.

17 (d) A person that provides notice under this section in
18 accordance with notification procedures developed and maintained
19 by the person pursuant to a security policy for the handling of
20 personal identifying information the person maintains is
21 considered to have complied with the notice requirements of this
22 section if the procedures are not inconsistent with the timing
23 requirements of this section.

24 (e) If the cost of providing written notice under this
25 section to all affected individuals would exceed \$250,000, the
26 number of affected individuals is more than 500,000, or the person
27 does not have sufficient contact information, the person may

1 provide for that notification by:

2 (1) sending an electronic mail message to an
3 individual's electronic mail address;

4 (2) posting a conspicuous statement of the occurrence
5 of the breach on the person's website; and

6 (3) notifying print or electronic media statewide that
7 a breach in the security of the person's computerized data system
8 has occurred.

9 (f) The notification required by this section may be delayed
10 at the request of a law enforcement agency conducting a criminal
11 investigation until the time that the law enforcement agency
12 determines that providing the notice will not impede the criminal
13 investigation.

14 (g) If a person becomes aware of circumstances that require
15 the person to notify more than 1,000 persons at any one time under
16 this section, the person shall also notify, without unreasonable
17 delay, each consumer reporting agency that compiles and maintains
18 consumer files on a nationwide basis of the timing, distribution,
19 and content of the required notices.

20 Sec. 50.004. DECEPTIVE TRADE PRACTICES. A violation of
21 this chapter is a false, misleading, or deceptive act or practice as
22 defined by Section 17.46(b) and is actionable by the consumer
23 protection division in a suit brought under Section 17.47.

24 Sec. 50.005. REMEDIES CUMULATIVE. The remedies provided by
25 this chapter are cumulative of any other remedy provided by law.

26 SECTION 2. This Act takes effect September 1, 2005.