BILL ANALYSIS

Senate Research Center
79R13594 CLG-F

H.B. 1682
By: McCall et al. (Shapleigh)
Business & Commerce
5/18/2005
Engrossed

AUTHOR'S/SPONSOR'S STATEMENT OF INTENT

Currently, no law exists in Texas requiring businesses that own or license data containing consumer personal information to notify customers when there has been a security breach. Recent security breaches include The University of Texas data system in 2002, which exposed more than 55,000 students, staff, and faculty to identity theft; The University of California data system in 2004, which exposed more than 1.4 million California residents to identity theft; and most recently ChoicePoint's data system in 2005, which exposed more than 145,000 Americans to identity theft. Legislation is needed to ensure that consumers receive notification of a security breach of their personal information, thereby allowing the consumers to take preventative measures.

H.B. 1682 requires businesses that own or license computerized data containing consumers' personal identifying information to disclose to affected residents of this state when there has been a breach in security of the data system. H.B. 1682 also provides that a violation of this Act constitutes a deceptive trade practice.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Title 4, Business and Commerce Code, by adding Chapter 50, as follows:

CHAPTER 50. DISCLOSURES RELATING TO MAINTENANCE OF PERSONAL IDENTIFYING INFORMATION

Sec. 50.001. DEFINITIONS. Defines "consumer reporting agency," "personal identifying information," and "service provider."

Sec. 50.002. BREACH OF SECURITY OF COMPUTERIZED DATA. (a) Sets forth the circumstances under which a breach in security of a person's computerized data system is considered to have occurred.

(b) Sets forth the circumstances under which access or acquisition of personal identifying information is not considered to be a breach in security of the person's system.

Sec. 50.003. NOTIFICATION OF SECURITY BREACH. (a) Requires a person that owns or licenses computerized data that includes personal identifying information of a resident of this state to notify the resident of any breach of the security of the person's computerized data system if the resident's unencrypted personal identifying information was, or may have been, obtained by an unauthorized person. Requires notification to be made promptly after the date the person discovers the security breach, taking into consideration any law enforcement agency requests as provided by Subsection (f) or any measures necessary to determine the scope of the breach or restore the reasonable integrity of the data system.

(b) Requires a service provider holding or using computerized data that includes unencrypted personal identifying information for a resident of this state to immediately notify and cooperate with the owner or licensee of the information of any breach of the security of the service provider's system if personal identifying information was, or may have been, obtained by an unauthorized person. Provides that the cooperation of a service provider with the owner or licensee of the information includes sharing information relevant to the breach.

(c) Requires the person, except as provided by Subsection (d) or (e), to provide notification required by this section in writing or by electronic notice, if electronic notice complies with certain requirements.

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

(e) Authorizes the person, under certain circumstances, to provide for notification by sending an electronic mail message, posting a conspicuous statement of the occurrence of the breach on the person's website, or notifying print or electronic media statewide that a breach in the security of the person's computerized data system has occurred.

(f) Authorizes the notification required by this section to be delayed at the request of a law enforcement agency conducting a criminal investigation until the time that the law enforcement agency determines that providing the notice will not impede the criminal investigation.

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

Sec. 50.004. DECEPTIVE TRADE PRACTICES. Provides that a violation of this chapter is a false, misleading, or deceptive act or practice and is actionable by the consumer protection division of the Office of the Attorney General.

Sec. 50.005. REMEDIES CUMULATIVE. Provides that the remedies provided by this chapter are cumulative of any other remedy provided by law.

SECTION 2. Effective date: September 1, 2005.