By: Elkins, Escobar, Crabb, Anderson, Leibowitz H.B. No. 3222

A BILL TO BE ENTITLED

AN ACT

relating to a business's duty to protect and safeguard sensitive personal information contained in its customer records.

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

SECTION 1. Section 48.102, Business & Commerce Code, as added by Chapter 294, Acts of the 79th Legislature, Regular Session, 2005, is amended to read as follows:

Sec. 48.102. BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION. (a) In this section:

(1) "Access device" means a card or device issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storing information. The term includes a credit card, debit card, or stored value card.

(2) "Breach of system security" has the meaning assigned by Section 48.103.

(3) "Financial institution" has the meaning assigned by 15 U.S.C. Section 6809.

(b) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

(c) A business that, in the regular course of business and in connection with an access device, collects sensitive personal

information or stores or maintains sensitive personal information in a structured database or unstructured files must comply with payment card industry data security standards.

(d) [~~(b)~~] A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means.

(e) A financial institution may bring an action against a business that is subject to a breach of system security if, at the time of the breach, the business is in violation of Subsection (c). A court may not certify an action brought under this subsection as a class action.

(f) Before filing an action under Subsection (e), a financial institution must provide to the business written notice requesting that the business provide certification or an assessment of the business's compliance with payment card industry data security standards. The certification or assessment must be issued by a payment card industry-approved auditor or another person authorized to issue that certification or assessment under payment card industry data security standards. The court shall, on motion, dismiss an action brought under Subsection (e) with prejudice to the refiling of the action if the business provides to the financial

institution the certification of compliance required under this subsection not later than the 30th day after receiving the notice.

(g) A presumption that a business has complied with Subsection (c) exists if:

(1) the business contracts for or otherwise uses the services of a third party to collect, maintain, or store sensitive personal information in connection with an access device;

(2) the business requires that the third party attest to or offer proof of compliance with payment card industry data security standards; and

(3) the business contractually requires the third party's continued compliance with payment card industry data security standards.

(h) A financial institution that brings an action under Subsection (e) may obtain actual damages arising from the violation. Actual damages include any cost incurred by the financial institution in connection with:

(1) the cancellation or reissuance of an access device affected by the breach;

(2) the closing of a deposit, transaction, share draft, or other account affected by the breach and any action to stop payment or block a transaction with respect to the account;

(3) the opening or reopening of a deposit, transaction, share draft, or other account affected by the breach;

(4) a refund or credit made to an account holder to cover the cost of any unauthorized transaction related to the breach; and

(5) the notification of account holders affected by the breach.

(i) In an action brought under Subsection (e), the court shall award the prevailing party reasonable attorney's fees and costs, except that a business may not be awarded reasonable attorney's fees and costs unless the court is presented proof that the business provided the certification or assessment of compliance with security standards to the financial institution within the period prescribed by Subsection (f).

(j) [~~(c)~~] This section does not apply to a financial institution, except that a financial institution that is injured following a breach of system security of a business's computerized data may bring an action under Subsection (e) and may be held liable for attorney's fees and costs for an action brought under that subsection as provided by Subsection (i) [~~as defined by 15 U.S.C. Section 6809~~].

SECTION 2. This Act takes effect January 1, 2009.