

By: Elkins

H.B. No. 345

A BILL TO BE ENTITLED

AN ACT

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

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

SECTION 1. Section 521.052, Business & Commerce Code, as effective April 1, 2009, is amended to read as follows:

Sec. 521.052. BUSINESS DUTY TO PROTECT 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 521.053.

(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 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

1 in a structured database or unstructured files must comply with
2 payment card industry data security standards.

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

7 (1) shredding;

8 (2) erasing; or

9 (3) otherwise modifying the sensitive personal
10 information in the records to make the information unreadable or
11 indecipherable through any means.

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

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

1 compliance required under this subsection not later than the 30th
2 day after receiving the notice.

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

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

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

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

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

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

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

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

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

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

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

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

17 SECTION 2. This Act takes effect January 1, 2011.