BILL ANALYSIS

Senate Research Center

H.B. 3222
By: Elkins et al. (Van de Putte)
Business & Commerce
5/18/2007
Engrossed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Recently, some large companies have suffered computer breaches of their networks that handle credit card, debit card, check, and merchandise transactions. Computer hackers have stolen an uncountable number of credit and debit card transactions that contain the cardholder's personal information. In one case, the hackers stole private information for years before the hacker's actions were detected.

Some companies store customer cardholder information in violation of Visa and MasterCard's Payment Card Industry Data Security Standards. Major credit card companies have launched security initiatives focused on businesses that store personal data. Unfortunately credit unions and banks are financially responsible for fraudulent transactions charged to members' accounts and are required to pay the costs of reissuing the cards to customers when a security breach occurs.

H.B. 3222 requires a business that collects personal information to use payment card industry data security standards to secure sensitive personal data.

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 Section 48.102, Business & Commerce Code, as added by Chapter 294, Acts of the 79th Legislature, Regular Session, 2005, as follows:

> Sec. 48.102. BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION. (a) Defines "access device," "breach of system security," and "financial institution."
>
> (b) Creates this subsection from existing text.
>
> (c) Requires 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 to comply with payment card industry data security standards.
>
> (d) Redesignated from existing Subsection (b).
>
> (e) Authorizes a financial institution to 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). Prohibits a court from certifying an action brought under this subsection as a class action.
>
> (f) Requires a financial institution, before filing an action under Subsection (e), to 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. Requires the certification or assessment to 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. Requires the court, on motion, to dismiss an action brought under Subsection (e) with prejudice to the refilling 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) Provides that a presumption that a business has complied with Subsection (c) exists under certain circumstances.

(h) Authorizes a financial institution that brings an action under Subsection (e) to obtain actual damages arising from the violation. Provides that actual damages include any cost incurred by the financial institution in connection with certain actions.

(i) Requires the court to award the prevailing party reasonable attorney's fees and costs in an action brought under Subsection (e), except that a business is prohibited from being 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) Redesignated from existing Subsection (c). Provides that 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 is authorized to 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), rather than providing that this section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

SECTION 2. Effective date: January 1, 2009.