SUBJECT: Business duty to protect and safeguard customer's personal information

COMMITTEE: Business and Industry — committee substitute recommended

VOTE: 7 ayes — Giddings, Elkins, Bailey, Castro, Martinez, Solomons, Zedler

0 nays

2 absent — Darby, Bohac

WITNESSES: For — Dale Kimble, Texas Credit Union League; (*Registered, but did not testify*: Steve Scurlock, Independent Bankers Association of Texas (IBAT)

Against — Chuck Gerard, Experian; Todd Baxter, Texas Cable and Telecommunications Association; (*Registered, but did not testify*: Vaughn Aldredge, AT&T; Jeffrey Clark, American Electronics Association; Cathy DeWitt, Texas Association of Business; James Hines, Verizon; Brad Shields, Texas Retailers Association Bryan Gonterman, AT&T Texas)

On — C. Brad Schuelke, Office of the Attorney General

BACKGROUND: Under Business and Commerce Code, secs. 48.102 and 48.103, a business must 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. A business must 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 shredding, erasing, or otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means. This section does not apply to a financial institution as defined by the federal Gramm-Leach-Bliley Act 15 U.S.C. sec. 2809.

Under sec. 48.103, a "breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person. Good faith acquisition of sensitive personal information by

an employee or agent of the person or business for the purposes of the person is not a breach of system security unless the sensitive personal information is used or disclosed by the person in an unauthorized manner.

Under sec. 48.201, a person who violates these provisions is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring suit to recover the civil penalty.

DIGEST:

CSHB 3222 would require a business that, in the regular course of business, collected, maintained, or stored sensitive personal information in connection with an access device to comply with payment card industry data security standards. The bill would define "access device" to mean a card or device issued by a financial institution that contained a magnetic stripe, microprocessor chip, or other means for storing information. The term would include a credit card, debit card, or stored value card.

CSHB 3222 would authorize a financial institution to bring an action against a business that was subject to a breach of system security if, at the time of the breach, the business did not comply with payment card industry data security standards. A court could not certify an action as a class action.

Before filing an action, a financial institution would have to provide to the business written notice requesting that the business provide certification of its compliance with payment card industry data security standards. The certification would have to be issued by a payment card industry-approved auditor within 90 days before a breech. Failure to provide certification would create a presumption of noncompliance. A court, on motion, would dismiss an action with prejudice if a business provided the certification to the financial institution 30 days after receiving the notice.

A presumption that a business had complied would exist if:

- the business contracted for or otherwise used the services of a third party to collect, maintain, or store sensitive personal information in connection with an access device;
- the third party was in compliance with payment card industry data security standards; and
- the business secured the third party's continued compliance with those standards.

The bill would permit a financial institution that brought an action to obtain actual damages arising from the violation and reasonable attorney's fees. Actual damages would include any cost incurred by the financial institution in connection with the breech involving cancellation or re-issuance of an access device, the closing of an account and any action to stop payment, the opening or reopening of an account affected, a refund or credit made to an account holder to cover the cost of an unauthorized transaction, and the notification of account holders.

The bill would take effect January 1, 2009.

SUPPORTERS SAY:

CSHB 3222 would require businesses that accepted credit, debit, or stored value cards to protect the cards' sensitive data using payment card industry data security standards (PCI DSS). These industry security standards have been agreed upon by five of the largest credit card entities: American Express, Discover, MasterCard, VISA, and JCB

The bill would address an expanding problem of businesses' failure to protect sensitive personal credit and debit card information. This problem came to national prominence in January with the revelation that hackers breeched credit card information from 45.7 million customers of T.J. Maxx and Marshall's stores. The hackers were able to obtain unencrypted credit card data as the stores processed electronic payments between the point-of-sale and banking networks.

When businesses sign up for Mastercard or VISA, they agree to follow PCI DSS, but estimates are that two-thirds of businesses that accept these cards are not compliant. By businesses not protecting sensitive personal information encoded on these cards, thieves fraudulently use the cards, creating millions of dollars of unnecessary losses.

CSHB 3222 would permit a financial institution to bring an action against a business that was subject to a breach of security if the business was not compliant with PCI DSS. The bill would not allow a class action.

The bill would create a safe harbor for business that complied with PCI DSS. It also would establish that businesses that used a third-party processor would be protected as long as the processor complied with PCI DSS.

CSHB 3222 would make businesses accountable for complying with PCI DSS as they agreed to when they contracted to conduct financial transactions with credit, debit, or stored value cards. By increasing incentives for compliance, the bill would decrease the risk of security breeches that could have an enormous adverse effect on both customers and financial institutions.

OPPONENTS SAY:

CSHB 3222 is not necessary because Texas already has a security breech notice law and a law requiring that businesses protect sensitive customer information. The bill would not be geared to customers but would create a new cause of action for financial institutions to sue other entities. Current case law allows a cause of action for negligence related to security breeches. In addition, the attorney general can bring suit to recover civil penalties under ch. 48.

OTHER OPPONENTS SAY:

Businesses providing customers a service should be allowed to retain personal financial information from credit and debit cards for a longer period than the industry standards prescribe in order to complete monthly automatic transactions or to offer certain services such as conducing billing transactions over the phone.