BILL ANALYSIS

C.S.H.B. 3222
By: Elkins
Business & Industry
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Some large companies have suffered computer breaches of their networks that handles 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 their 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 must pay to reissue cards to customers when a security breach occurs.

C.S.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

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.H.B. 3222 amends the Business and Commerce Code to define the terms "access device", "breach of system security", and "financial institution".

C.S.H.B. 3222 requires a business, in the regular course of business that collects, maintains, or stores sensitive personal information in connection with an access device, to follow payment card industry data security standards. The bill authorizes a financial institution to bring an action against a business which is subject to a security breach if, at the time of the security breach, the business is in violation of certain provisions of the bill. The bill prohibits a court from certifying an action brought under this bill as a class action. The bill requires a financial institution to provide to the business written notice requesting the business to provide certification of the business's conformity with payment card industry data security standards, before filing an action. The bill requires the certification to be issued by a payment card industry-approved auditor no earlier than the 90th day before the date of the security breach. The bill requires the court, on motion, to dismiss an action brought with prejudice to the refiling of the action if the business presents to the financial institution the required compliance certification no later than the 30th day after receiving the notice. The bill provides that failure to provide the certification creates a presumption of noncompliance with payment card industry data security standards.

C.S.H.B. 3222 adds that a presumption that a business has complied with provisions of the bill exists if the business contracts or uses the services of a third party to maintain, collect, or store sensitive personal information in connection with an access device; the third party is in compliance with payment card industry data security standards; and the business assures the third party's continued compliance with those standards.

C.S.H.B. 3222 authorizes a financial institution that brings an action to obtain actual damages arising from the violation and reasonable attorney's fees. The bill sets forth that what is to be included in actual damages awarded in an action.

C.S.H.B. 3222 exempts a financial institution from the provisions of the bill. The bill authorizes a financial institution that is injured following a breach of system security of a business's computerized data to bring an action.

EFFECTIVE DATE

January 1, 2009.

COMPARISON OF ORIGINAL TO SUBSTITUTE

The substitute differs from the original by adding a definition for "access device". The substitute modifies the provision that a business that collects, maintains, or stores sensitive personal information in connection with an access device is required to comply with payment card industry data security standards. The substitute clarifies that a financial institution is authorized to bring an action against a business if the business is in violation of compliance with payment card industry data security standards. The substitute clarifies that a court is prohibited from certifying a class action.

The substitute adds language that states the actions that a financial institution is required to take before filing an action. The substitute requires the court, on motion, to dismiss an action if the business provides certification of compliance. The substitute states that the failure to provide certification creates a presumption of noncompliance. The substitute lists the standards in which a business has complied with the provisions of the bill.

The substitute amends Section 48.102, Business and Commerce Code, to add language that a financial institution that brings an action is authorized to obtain actual damages arising from the violation and lists the costs incurred by the financial institution that are authorized to be considered in actual damages.