BILL ANALYSIS

C.S.H.B. 345
By: Elkins
Business & Industry
Committee Report (Substituted)

BACKGROUND AND PURPOSE

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 undeterminable number of credit and debit card transactions that contain the cardholder's personal information. In one case, hackers stole private information for years before the hackers' 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.

C.S.H.B. 345 requires a business that stores sensitive personal information derived from an access device to reasonably protect such information against unauthorized access or use. The bill authorizes the attorney general to bring an action against a business that is subject to a breach resulting from the business' failure to reasonably protect such information.

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. 345 amends the Business & Commerce Code to require a business that stores sensitive personal information derived from a credit card, debit card, stored value card, or other access device issued by a financial institution to reasonably protect such information against unauthorized access or use. The bill makes a business that fails to reasonably protect such information liable to the state for a civil penalty and authorizes the attorney general in bringing action to recover the penalty, if such failure results in a breach of a security system, to seek any order or judgment necessary to compensate a financial institution from actual damages resulting from the breach, including reasonable costs incurred by the institution in connection with certain actions taken by the financial institution to manage, restore, or close an account affected by the breach. The bill defines the term "access device."

EFFECTIVE DATE

January 1, 2011.

COMPARISON OF ORIGINAL AND SUBSTITUTE

C.S.H.B. 345 differs from the original by requiring a business that stores sensitive personal information derived from an access device to reasonably protect such information against unauthorized access or use, whereas the original requires the business to comply with payment card industry data security standards. The substitute removes provisions in the original relating to a business' compliance with such standards.

C.S.H.B. 345 adds a provision not in the original making a business that fails to reasonably protect personal information derived from an access device liable to the state for a civil penalty. The substitute differs from the original by authorizing the attorney general in bringing action to collect the civil penalty to seek compensation for an affected financial institution if the business' failure to reasonably protect such information results in a breach of system security, whereas the original authorizes a financial institution to bring an action against and obtain damages from such a business, sets out procedures for such an action, and limits an award to the prevailing party.

C.S.H.B. 345 specifies that reasonable costs, rather than any costs as in the original, incurred by an affected financial institution in connection with certain actions taken by the institution to manage or restore an account affected by a breach are authorized to be recovered as damages.

C.S.H.B. 345 removes definitions in the original for "breach of security system" and "financial institution."