BILL ANALYSIS

C.S.H.B. 2138
By: Hopson
Financial Institutions
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Credit card "skimming" is a method by which information encoded in a magnetic strip of a credit card is gathered by an electronic card reader, or skimmer. This information is used legitimately when processing a credit card transaction. However, a skimmer can become a handy tool for criminals who use the skimmed data for illegal transactions and purchases or to re-encode the magnetic strip of a counterfeit card.

C.S.H.B. 2138 would create an offense for a person who uses a skimmer or re-encoder to access, read, scan, store, or transfer the information encoded on a payment card's magnetic strip without the consent of the card's authorized user.

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. 2138 adds new Section 35.38, Business & Commerce Code to provide that a person commits an offense by using a scanning device or re-encoder to access, read, scan, store, or transfer information encoded on the magnetic strip of a payment card without the consent of the card's authorized user and with intent to harm or defraud another. Such an offense is a Class B misdemeanor (up to $2,000 fine and/or up to 180 days in jail). However, the perpetrator may be prosecuted under another law if the action triggering this bill's provisions also constitutes another offense.

The bill provides definitions for "payment card," "re-encoder," and "scanning device," and makes conforming changes to the Code of Criminal Procedure.

EFFECTIVE DATE

September 1, 2003

COMPARISON OF ORIGINAL TO SUBSTITUTE

The substitute adds the provision permitting the prosecution of another offense in lieu of prosecuting for an offense established by the bill.