

## **BILL ANALYSIS**

S.B. 2371  
By: Nichols  
Pensions, Investments & Financial Services  
Committee Report (Unamended)

### **BACKGROUND AND PURPOSE**

The 87th Texas legislature passed H.B. 2106, which gave the Texas Department of Licensing and Regulation rulemaking authority with regard to legislative and law enforcement efforts in preventing the installation of card skimmers on gas pumps. The bill created the Financial Crimes Intelligence Center (FCIC) to enhance coordination of law enforcement strategies for combatting organized financial crimes resulting from the proliferation of card skimmers at gas pumps. The bill sponsor has informed the committee that, despite the FCIC's original mission to prevent card skimming, the rise of transnational criminal activities and the proliferation of new electronic payment devices have emphasized the need to expand the FCIC's authority to address these evolving threats and to subject different types of electronic terminals to that authority. S.B. 2371 seeks to build on existing strategies for fighting these types of financial crimes by targeting crimes occurring through a broader range of devices, providing for civil and criminal penalties to give law enforcement more tools to fight these crimes, and expanding the scope of the FCIC's authority to include oversight of certain electronic terminals, such as ATMs, point-of-sale terminals, and virtual currency kiosks.

### **CRIMINAL JUSTICE IMPACT**

It is the committee's opinion that this bill expressly does one or more of the following: creates a criminal offense, increases the punishment for an existing criminal offense or category of offenses, or changes the eligibility of a person for community supervision, parole, or mandatory supervision.

### **RULEMAKING AUTHORITY**

It is the committee's opinion that rulemaking authority is expressly granted to the financial crimes intelligence center in SECTION 1 of this bill.

### **ANALYSIS**

S.B. 2371 amends the Business & Commerce Code to establish provisions relating to payment card skimmers on electronic terminals.

#### **Duties for Use of Certain Electronic Terminals**

##### **Required Notice of Skimmer Discovery**

S.B. 2371 requires a service technician or the service company that employs the technician that discovers a skimmer in or on an electronic terminal, to notify the financial crimes intelligence center and the merchant of the skimmer in the manner prescribed by center rule. The bill requires a merchant, if the merchant discovers a skimmer in or on an electronic terminal or is notified of the presence of a skimmer, to do the following in the manner prescribed by center rule:

- disable, or cause to be disabled, the electronic terminal on which the skimmer was discovered;

- notify a law enforcement agency and the center that a skimmer has been detected; and
- take appropriate measures to protect the electronic terminal from tampering until the center or law enforcement agency arrives and the skimmer is removed.

#### Report to Center and Investigation of Skimmer Report

S.B. 2371 authorizes the financial crimes intelligence center to accept a report of a suspected skimmer from any interested person, including a law enforcement agency, a financial institution, a payment card issuer, a service technician or service company, a member of the public, and a payment card network. The bill authorizes the center, on receipt of a report of skimming or suspected skimming, to conduct an inspection for the presence of suspected skimmers. The bill requires the center to coordinate with law enforcement agencies in conducting the investigation of such reports. The bill authorizes the center, if a skimmer is reported to be located on an electronic terminal, to inspect, directly or in coordination with a law enforcement agency, the electronic terminal that is the subject of the report and any other electronic terminal located at the same place of business. The bill requires a merchant to cooperate with the center or a law enforcement agency during an investigation of a skimmer discovered or reported at the merchant's place of business and to allow the inspection and alteration of an electronic terminal at the place of business as necessary.

#### Confidentiality

S.B. 2371 establishes that the following information is confidential and not subject to disclosure under state public information law:

- information from a report received by the financial crimes intelligence center under the bill's provisions; or
- information prepared or compiled by the center in connection with the report or an investigation.

However, the bill subjects such information to disclosure under state public information law on the dismissal or final resolution of a report by the center, unless the information is subject to statutory provisions relating to prohibited disclosure by the Texas Department of Banking or can be classified as confidential information under applicable rules.

Additionally, S.B. 2371 authorizes the information to be disclosed to the following entities:

- a public institution of higher education;
- a law enforcement agency;
- a payment card issuer, a financial institution that is not a payment card issuer, or a payment card network that may be impacted by the use of a skimmer on an electronic terminal;
- another person if the disclosure of the information is authorized or required by other law or court order;
- a trade association representing a financial institution;
- a center contractor or other agent; or
- the Texas Department of Banking.

The disclosure of such information to these entities is not a voluntary disclosure for purposes of applicable Government Code provisions. The bill authorizes a law enforcement agency or the center to disclose to the public information made confidential under the bill's provisions if the law enforcement agency or the chief intelligence coordinator for the center determines the disclosure of the information furthers a law enforcement purpose. However, the bill prohibits a law enforcement agency or the center from disclosing to the public the identity of a person who submits a report of a suspected skimmer to the center.

## **Enforcement**

### Civil Penalty

S.B. 2371 makes a person who violates the bill's provisions or a rule adopted under the bill's provisions liable to the state for a civil penalty. The bill caps the civil penalty at \$5,000 per day for each violation and authorizes the attorney general to bring an action to collect the civil penalty. The bill requires an action filed under these provisions to be filed in a district court in Travis County. The bill authorizes the attorney general and the department to recover reasonable expenses incurred in obtaining injunctive relief, including court costs, reasonable attorney's fees, investigative costs, witness fees, and deposition expenses.

### Criminal Offenses

S.B. 2371 creates the following offenses:

- a Class C misdemeanor offense for a person who refuses to allow an inspection of an electronic terminal at the merchant's place of business in violation of the bill's provisions;
- a Class B misdemeanor offense for a person who negligently or recklessly disposes of a skimmer that was installed on an electronic terminal by another person; and
- a third degree felony offense for a person who, knowing that an investigation is ongoing or that a criminal proceeding has been commenced and is pending, disposes of a skimmer installed on an electronic terminal by another person.

### Applicability and Enforcement; Rules

S.B. 2371 requires the financial crimes intelligence center to administer and enforce the bill's provisions and to adopt rules for administering the bill's provisions.

## **Definitions**

S.B. 2371 defines the following terms for purposes of the bill's provisions:

- "automated teller machine" by reference to Penal Code provisions relating to theft;
- "electronic terminal" as an electronic device, other than a telephone operated by a consumer, through which a consumer may initiate an electronic funds transfer, including a point-of-sale terminal, virtual currency terminal, automated teller machine, and cash dispensing machine;
- "financial institution" by reference to Finance Code provisions relating to business checking accounts;
- "institution of higher education" by reference to Education Code provisions relating to the Texas Higher Education Coordinating Board;
- "merchant" by reference to the Uniform Commercial Code--Sales;
- "payment card" by reference to statutory provisions relating to identity theft by an electronic device;
- "payment card issuer" as a lender, including a financial institution, or a merchant that receives applications and issues payment cards to individuals;
- "payment card network" as an entity that directly, or through a licensed member, processor, or agent, provides the proprietary services, infrastructure, and software that route information to conduct debit card or credit card transaction authorization, clearance, and settlement and which the entity uses to accept as a form of payment a brand of debit card, credit card, or other device to be used to carry out debit or credit transactions;
- "service company" and "service technician" by reference to Occupations Code provisions relating to the licensing of motor fuel metering device service technicians and motor fuel metering device service companies;

- "skimmer" as a wire or electronic device capable of unlawfully intercepting electronic communications or data to perpetrate fraud; and
- "virtual currency" as an intangible electronic medium of exchange, unit of account, or store of value.

**EFFECTIVE DATE**

On passage, or, if the bill does not receive the necessary vote, September 1, 2025.