SUBJECT: Requiring pawnshops to transfer data electronically to law enforcement

COMMITTEE: Financial Institutions — committee substitute recommended

VOTE: 6 ayes — Solomons, Gutierrez, Flynn, Hopson, Paxton, Wise

0 nays

1 absent — Christian

WITNESSES: For — Harry Griffin, San Antonio Chief of Police

Against — Thomas Elliott, Dallas Police Department; G. Ermis, Corpus Christi Police Department

On — W.J. Mike Murphy, Texas Association of Pawn Brokers; Leslie Pettijohn, Consumer Credit Commissioner; Bill White, Cash America International, Inc.; *(Registered, but did not testify:)* Michael O. Sullivan, l.e.a.d.s online

BACKGROUND: Finance Code, ch. 371 governs pawnshops under regulation of the Office of the Consumer Credit Commissioner (OCCC). Sec. 371.204 allows law enforcement officers access to pawnshop records. Pawnshops share transaction data with law enforcement in different ways to facilitate the investigation of alleged property crimes. About 8 percent of pawnshops keep only handwritten records, while the remainder are computerized to varying degrees. Some private vendors also collect pawnshop data and offer it as a product to law enforcement entities. About 25 percent of law enforcement jurisdictions in Texas report that they can receive electronic data from pawnshops. Those who cannot receive electronic data gather pawnshop records and enter the data manually into their computer systems.

The 77th Legislature in 2001 enacted HB 1763 by McCall, et al. requiring the Finance Commission and the Department of Information Resources to form a committee to devise a standard format for pawnbrokers to provide data electronically to law enforcement agencies and to explore related privacy issues. The committee issued a report to the Legislature in June 2002.

DIGEST:

CSHB 1839 would authorize a county sheriff or city police chief to place a hold order on goods held by a pawnbroker if the officer reasonably suspected that the goods had been stolen or otherwise misappropriated. The pawnbroker would have to retain the goods until the order expired, was released, or overturned by a court order. The bill would specify contents of a hold order and would establish an initial holding period of up to 60 days that could be extended for up to three successive 60-day periods, or 180 days in all, by written notification. The officer could place a verbal hold order on property for up to seven days while a written hold order was being prepared.

Goods subject to a hold order could be released to the officer's custody for use in a criminal investigation if the officer furnished a written receipt for the goods. Release of the goods would not be considered a waiver of the pawnbroker's rights or interest in the goods.

A person who pledged misappropriated property with a pawnbroker or sold such property to a pawnbroker would commit a Class B misdemeanor, punishable by up to 180 days in jail and/or a maximum fine of $2,000.

Electronic data transfer. The bill would define reportable data distinctly from transaction data. Both would include the pawnshop's name and address, date of transaction, and identification of the good pledged or sold, including model or serial numbers. Transaction data also would include identifying information about the customer, including name, address, physical description, and driver's license or other identification number.

A pawnbroker who generated computerized pawn and purchase tickets would have to transmit electronically either reportable data to a law enforcement agency or transaction data to a third-party provider within seven days of the transaction, if so required by the chief law enforcement officer. A pawnbroker also could transmit transaction data to law enforcement by other mutually agreed upon means. Law enforcement and third-party providers would have to maintain security for the data with at least 128-bit encryption and could not charge a fee to pawnbrokers or pawn customers for this service.

A third-party provider could establish a repository for transaction data and could charge law enforcement agencies a reasonable fee for access to the data. The provider would have to update the repository daily and secure it against

access from anyone other than designated law enforcement officials. The repository would have to enable pawnbrokers to transmit data over the Internet and enable authorized law enforcement officers to obtain the data over the Internet by using an access code or other security device.

If law enforcement officers wanted to obtain the identity of a customer in a pawn transaction, they would have to represent that they sought information in connection with a criminal investigation and present either the investigation case number or their name and badge number. The repository also would have to record the name of the law enforcement officer, the pawn transaction, and the identity of any customer identified in every search conducted. All data in the repository would be confidential. The bill would establish a Class A misdemeanor (punishable by up to one year in jail and/or a maximum fine of $4,000) for disclosing data in violation of this provision and for fraudulent access to a repository.

The consumer credit commissioner could require documentation of a provider's or law enforcement agency's compliance with these statutes. Each provider and law enforcement agency that collected electronic data would have to report the annual number of transactions reported by each pawnbroker to the commissioner by January 31 of each year.

Pawnbrokers could not be held responsible for delays in electronic data submission caused by computer-related malfunctions of the provider's or law enforcement agency's computer equipment, or, in some circumstances, of their own equipment. For 180 days after a pawnshop began electronic data transfer, and following any computer malfunction, the pawnshop would have to make paper copies of transaction documents available to law enforcement. The Finance Commission could adopt rules to address computer-related malfunctions and errors and paperwork requirements.

The bill would take effect January 1, 2004.

SUPPORTERS SAY:

Existing rules for electronic data transfer (EDT) help with investigation of property crimes, but they create inefficiencies for law enforcement agencies that have to sort through paper copies of pawn transaction data to locate the very small minority of pawn transactions associated with stolen property. This often is a labor-intensive process whose diligence can suffer in jurisdictions

with few resources or other priorities. Law enforcement has wanted change in this area for a long time, and CSHB 1839 would provide it.

Pawnshops suffer from the popular misconception that their customers are either criminal or otherwise on the fringe of society. However, reputable people commonly use pawnshops in times of financial hardship. Pawnshops' transaction data thus represents a collection of personal financial data primarily from law-abiding persons — *not* a criminal database. Existing rules are problematic because law enforcement officials have unrestricted access to pawn transaction data with no guidelines about what they may or may not do with the data. Given the history of some law enforcement officials using pawn data for profiling and inappropriate data mining, CSHB 1839 would protect personal financial data from being used in such discriminatory ways.

The bill would enable a law enforcement agency to receive reportable data, omitting customer identification information, directly from pawnshops. It also would allow, but not require, pawnbrokers to transmit transaction data, including customer identification information, to law enforcement officials. Some larger jurisdictions already have a good methodology in place for using EDT with transaction data, and it is not the bill's intent to disturb systems that work well. Law enforcement agencies now have access to customer identity information in pawn transaction records, but the bill would limit the data they could demand from pawnbrokers to reportable data, with the intention of protecting privacy rights.

Alternatively, the bill would allow a sheriff or police chief to direct a pawnshop to report transaction data, including the customer's identification information, directly to a third-party provider, who then would allow law enforcement to access customer identity data under certain conditions when investigating a crime. This combination of options would strike a good balance between protecting privacy rights and aiding law enforcement investigations. It also would allow cities and counties the flexibility to choose what was best for their jurisdictions. The bill would avoid imposing electronic reporting requirements on pawnshops who did not have the technology necessary for electronic reporting.

It is important not to require the use of a third-party provider. Doing so could create a monopoly intermediary between pawnshops and law enforcement,

especially if the requirement were accompanied by formatting specifications tailored to favor a certain company. The Legislature should not create monopolies or any new market not likely to be fully competitive. Rather, it should encourage agreement and cooperation directly between pawnshops and law enforcement.

Hold procedures specified by the bill would replace the current piecemeal system of holds with a consistent procedure across jurisdictions. With two 60-day extensions available, the term of property holds would be sufficient to accommodate most jurisdictions' investigation workload and timing.

OPPONENTS SAY:

No governmental entity should be allowed to hold pawn transaction data, because it contains the financial data of law-abiding private people who use property as collateral for loans, not mass information about criminals.

The bill would allow sheriffs and police chiefs to decide whether to require EDT from pawnshops directly or through a third-party provider. The privacy rights of taxpayers would be better protected by requiring the use of a third-party provider without giving sheriffs and police chiefs the discretion to house the data within their departments.

OTHER OPPONENTS SAY:

CSHB 1839 actually could reduce law enforcement's access to data by restricting their ability to conduct customer name searches. Law enforcement officials now can obtain customer names in pawn transaction records, which is of great assistance when the only information law enforcement has about a crime is the name of the suspect. This level of access is necessary to ensure vigorous enforcement of property rights for those whose property has been stolen.

If one of the goals of this bill is to help law enforcement investigate property crimes, the Department of Public Safety (DPS) should be the repository of statewide pawnshop data, not private-sector companies or local law enforcement agencies. A statewide database under DPS would ease cross-jurisdictional investigations and would reflect the reality that a local system does nothing to prevent a criminal from pawning stolen property in a neighboring jurisdiction. DPS' experience in administering the statewide database for criminal background checks would be an asset in administering

the pawn records database, particularly because of the security concerns involved in maintaining such sensitive personal data.

NOTES:

The committee substitute added the section relating to hold procedures; allowed the submission of data electronically to a third-party, specified provider and repository requirements; defined the data to be transmitted; set procedures to follow during computer malfunctions; allowed oversight by the consumer credit commissioner; authorized the Finance Commission to adopt rules for implementation; removed formatting specifications for electronic data transmission; deleted a requirement that law enforcement agencies destroy data within seven days of receipt; increased the number of days within which a pawnbroker would have to transmit data; and changed the effective date.