SUBJECT: Prevention, prosecution, and punishment of identity theft

COMMITTEE: Criminal Jurisprudence — committee substitute recommended

VOTE: 7 ayes — Keel, Riddle, Denny, Ellis, Hodge, Pena, Talton

0 nays

2 absent — Dunnam, P. Moreno

SENATE VOTE: On final passage, April 2 — voice vote

WITNESSES: For — Merry Lynn Gerstenschlager, Texas Eagle Forum; George May, Yellow Rose Mortgage Company; Luke Metzger, Texas Public Interest Research Group; Karen Neeley, Independent Bankers Association of Texas; Rob Schneider, Consumers Union; Matt Wilson

Against — Chuck Courtney, Texas Retailers Association; Stuart Pratt, Consumer Data Industry Association; Brad Shields

On — George Cervantes, Texas Association of Licensed Investigators; John Chism, Texas Association of Licensed Investigators; Raika Hammond, Texas Municipal League; David Mintz, Texas Apartment Association; Daniel Nestel, Reed Elsevier/LexisNexis

BACKGROUND: Penal Code, sec. 32.51, makes it a state-jail felony (180 days to two years in a state jail and an optional fine of up to $10,000) to obtain, possess, transfer, or use identifying information of another person without consent and with intent to harm or defraud another. If a court orders a defendant convicted of an offense to make restitution to the victim, the court may order the defendant to reimburse the victim for lost income or other expenses, other than attorney's fees, incurred as a result of the offense. Identifying information means information that alone, or in conjunction with other information, identifies an individual, including an individual's:

- name, social security number, date of birth, and government-issued identification number;

- unique biometric date, including the individual's fingerprint, voice print, and retina or iris image;
- unique electronic identification number, address, and routing code; and
- telecommunication identifying information or access device, which means a card, code, account number, etc., that may be used to obtain money, goods, services, or other things of value, or to initiate a transfer of funds other than a transfer originated solely by paper instrument.

Government Code, ch. 552, the Public Information (open records) Act, requires public information to be available to the public during normal business hours of the governmental body. Information is considered public information if, under a law or ordinance or in connection with the transaction of official business, it is collected or maintained by a governmental body or for a governmental body that owns the information or has a right of access to it. The Public Information Act excludes certain information from required disclosure, including information considered to be confidential by law. A governmental body that receives a written request for information that it wishes to withhold from public disclosure and that it considers to be within a valid exception must ask for a decision from the attorney general about whether the information falls within that exception.

Business and Commerce Code, ch. 20, regulates consumer credit reporting agencies.

DIGEST:

Protection of consumer information. The bill would add provisions to Business and Commerce Code, ch. 20, to require a consumer reporting agency to follow reasonable procedures in preparing or disseminating information to ensure maximum possible accuracy of the information about the consumer.

Further, if a person requested a consumer report from an agency and the request included an address for the consumer that substantially differed from the address in the consumer file, the agency would have to notify the requestor, before or at the time of providing the consumer report, that the addresses were different. That requirement only would apply to an agency that maintained a database to produce consumer reports that included public record information and credit account information compiled from information furnished by persons regularly and in the ordinary course of business.

Identity theft. The bill would add provisions to the Business and Commerce Code to create the following offenses and remedies.

Offenses. A person could not obtain, possess, transfer, or use personal identifying information of another person without that person's consent and with fraudulent intent to obtain a good, service, insurance, an extension of credit, or any other thing of value. Personal identifying information would have the same definition as in Penal Code, sec. 32.51, described above, except that it also would include a mother's maiden name and would apply to information used to identify a dead individual.

A business would have to implement and maintain reasonable procedures to prevent the unlawful use of any personal identifying information collected or maintained by the business. This provision would not apply to a financial institution.

A person that engaged in business with another person who allegedly used the consumer's personal identifying information would have to disclose without charge to the consumer or a peace officer, upon request, not later than the 30th business day after receiving the request:

- a copy of any application or transactional information related to an alleged violation of Penal Code, sec. 32.51; and
- the personal identifying information of the consumer that the person who allegedly impersonated the consumer used, or information related to the use of that information.

Before disclosing that information, the person could require the consumer to submit a signed and dated written authorization with specified information. A person could not be held liable for failure to disclose the information to a peace officer because a consumer failed to provide the authorization requested.

A credit card issuer who received a request for a change of billing address and received, before the 11th day after the date of the first request, a request for an additional credit card on the same account could not mail the card to the new address or activate the card unless the credit card issuer verified the change of address.

A person would commit a state-jail felony by using a scanning device or re-encoder to access, scan, store, or transfer information encoded on the magnetic strip of a payment card without the consent of an authorized user and with intent to harm the user. Re-encoder would mean an electronic device that can be used to transfer encoded information from a magnetic strip on a payment card onto the magnetic strip of a different payment card.

Remedies. A person who violated the above provisions would be liable for a civil penalty of at least $2,000 but not more than $50,000 for each violation in a suit brought by the attorney general. Furthermore, the attorney could bring an action for a temporary restraining order or a permanent or temporary injunction to prevent a person from engaging in conduct that violated the provisions. The action for a restraining order or injunction could be brought in any county where the violation occurred, Travis County, or the county in which the victim resided. The court could grant any other equitable relief that it considered appropriate to prevent any additional harm to a victim of identity theft or to satisfy a judgement entered against the defendant.

A person who accepted a debit or credit card for the transaction of business could not print more than the last four digits of the account number or the month and year of the card's expiration date on a receipt. A violator would be liable to the state for a civil penalty not to exceed $500 for each month during which a violation occurred, and the attorney general or prosecuting attorney in the county in which the violation occurred could bring suit. The attorney general also could bring an action to restrain or enjoin a person from violating the provisions. A court could not certify such an action as a class action suit. Finally, the requirements would not apply to a transaction in which the sole means of recording a person's debit or credit card account number on a receipt was by handwriting or by an imprint or copy of the card.

The attorney general would be entitled to recover reasonable expenses including reasonable attorney's fees and court costs, as well as restitution for a victim. Penalties collected would have to be deposited in the general revenue fund and only could be appropriated for the investigation and prosecution of identity theft cases.

A person who was injured by one of the violations listed above, other than the section governing the disclosure of information to a consumer, or who filed a

criminal complaint alleging a commission of an offense under Penal Code, sec. 32.51, could file an application with a district court for the issuance of a court order declaring that the person was a victim of identity theft. After notice and a hearing, if the court was satisfied by a preponderance of the evidence that the applicant was injured by a violation of these provisions, the court would have to enter an order containing a declaration that the person was a victim of identity theft, any known information identifying the violator, information identifying any financial account or transaction affected by the violation, and the specific personal identifying information used to commit the alleged violation. The order would have to be sealed and only could be released in limited circumstances. Further, a court could vacate an order if it found that the application or any information submitted to the court by the applicant contained a fraudulent or material misrepresentation.

A violation of the above provisions, other than the section governing the disclosure of information to a consumer, would be a deceptive trade practice.

Good faith reliance on a consumer report by a financial institution would be an affirmative defense to an action brought against the financial institution under any of the provisions above.

Disposition of contraband. The bill would amend Code of Criminal Procedure, art. 18.18, to include scanning devices and re-encoders among the list of contraband that must be destroyed or forfeited following conviction of certain crimes or a hearing on the issue.

Driver's license offense. The bill would amend the Transportation Code to make it a class A misdemeanor (up to one year in jail and/or a maximum fine of $4,000) to knowingly access or use electronically readable information from a driver's license or personal identification certificate, or knowingly compile or maintain a database of electronically readable information from driver's licenses or personal identification certificates. However, the prohibition would not apply to a Department of Public Safety (DPS) employee or officer, a peace officer, a licensed Parks and Wildlife deputy, or a person complying with the Alcoholic Beverage Code, or a financial institution in some instances.

Law enforcement guidelines. The bill would require a peace officer who received a report of identity theft under Penal Code, sec. 32.51, to make a written report including the name of the victim and suspect, if known, the type of identifying information obtained or used, and the results of the investigation. Upon request, the peace officer would have to provide the victim with the report, after redacting confidential information other than that described above.

An offense under Penal Code, sec. 32.51, could be prosecuted in any county where the identifying information was obtained or used, or the county of residence of the victim. Also, a court could order the defendant to reimburse the victim for lost income or other expenses, including attorney's fees.

The bill would include persons who are victims of fraudulent use or possession of identifying information in the definition of victim in the Code of Criminal Procedure, for purposes of certain crime victims' rights. Those rights include the right to receive from law enforcement adequate protection from harm and threats of harm arising from cooperating with the prosecution, the right to be informed of relevant court proceedings and the defendant's right to bail, among others.

The bill would amend the Government Code to require the director of the DPS to create an identity theft unit that would:

- encourage local law enforcement agencies to file a report with DPS immediately on receipt of a complaint alleging identity theft;
- assist a local law enforcement agency that requested help in the investigation of a complaint alleging identity theft; and
- initiate an investigation on receipt of reports from two or more local agencies that appeared to involve the same offender.

The Commission on Law Enforcement Officer Standards and Education would have to establish a statewide comprehensive education and training program on identity theft, and an officer would have to complete the program not later than the second anniversary of the date the officer was licensed, and as a requirement for an intermediate proficiency certificate.

Confidentiality of personal information in government records. The bill would amend the Government Code to prevent a state or local governmental entity from disclosing the following information to a member of the public and to require the entity to redact the information from a document made available to the public:

- information that reveals an individual's social security number or passport number;
- an individual's bank account, credit card, or debit card number, or other financial account number; or
- an individual's computer password or access code, or computer network location or identity.

This requirement would not apply to information including court records, historical documents, information collected by the Texas Department of Criminal Justice (TDCJ) or the Texas Youth Commission (TYC) about an offender, or personal information relating to a motor vehicle accident. The term governmental entity would not include a court other than a commissioners court. Further, the governmental entity could disclose the information to another state or local governmental entity in Texas, a federal governmental entity, or a private investigator, among others.

A governmental entity would not be required to request a decision of the attorney general before refusing to disclose the information. In responding to an open records request for a document that contained that information, the governmental body would have to inform the person making the request that the information was being redacted. The person could complain to the attorney general that the governmental entity withheld information other than the personal information required to be redacted, and the attorney general could review that matter. If the attorney general determined that the governmental body redacted information other than the personal information described above, the Public Information Act would apply to that information.

A state or local governmental entity would have to establish procedures to ensure that it collected personal information only to the extent reasonably necessary to implement a program, authenticate an individual's identity, ensure security, or accomplish another legitimate governmental purpose. Furthermore, in adopting or amending its records retention schedule, a

governmental entity would have to schedule the retention of personal information only for the period necessary to accomplish the purpose for which the information was collected or the minimum period prescribed by statute.

In addition, the bill would require governmental entities to develop a written privacy policy describing the reasons for collecting each category of personal information, the persons to whom the information could be disclosed, the manner of disclosure, and the manner in which a member of the public could protect private information by redacting or omitting it, among other things. The Department of Information Resources would have to adopt rules prescribing minimum privacy standards with which an Internet site maintained by or for a state governmental entity would have to comply.

The state auditor would be required to establish auditing guidelines to ensure that a governmental entity routinely did not collect or retain more personal information than necessary, and had established an information management system that protects the privacy and security of information in accordance with state and federal law.

The attorney general would have to establish guidelines for governmental entities to follow when considering privacy and security issues that arise in connection with requests for public information. The guidelines would have to balance the need for open government with respect for personal privacy and the security needs of the state.

In addition, the bill would contain the following provisions:

- requiring the open records steering committee periodically to study the implications of putting information held by government on the Internet and to include its findings and recommendations in reports;
- requiring the Records Management Interagency Coordinating Council to provide guidance to local governmental entities in incorporating developments in electronic management into their information management systems to protect personal privacy; and
- amending the Property Code to require instruments executed on or after January 1, 2004, transferring an interest in real property to include a notice that a person could strike a social security or driver's license number from the instrument before filing it.

The bill would take effect on September 1, 2003, except that the provisions relating to the establishment of an identity theft unit would not take effect until September 1, 2005, and the provisions relating to the confidentiality of governmental records would not take effect until January 1, 2004 for municipalities with populations of less than 1.2 million.

SUPPORTERS SAY:

CSSB 405 would help combat identity theft within Texas. Identity theft is the fastest growing crime in the United States. It occurs when a perpetrator uses another person's name, address, social security number, or other identifying information to establish credit, run up debt, or take over financial accounts. Identity thieves use a variety of methods, including watching from a distance as a victim enters credit card numbers, eavesdropping on conversations, obtaining personal identification information by looking through phone records or bank statements in the trash, calling the victim and pretending to be a bank or other organization, or swiping a credit card through an unauthorized handheld reader. Furthermore, thousands of stolen credit card numbers are sold on the Internet.

A long period of time typically passes before a victim notices the crime. As a result, the victim's credit report might contain fraudulent charges, which could result in the victim being unable to obtain credit and financial services, telecommunication and utility services, and even employment. In the worst case scenario, an identify thief might create a criminal record in the victim's name that could cause the victim to have a driver's license revoked, fail background checks, and even be arrested. It not only affects consumers but costs financial institutions and retail stores a great deal of money every year.

Protection of consumer information. The bill would impose reasonable requirements on businesses that would go a long way toward protecting consumers' identifying information. Consumer reporting agencies would have to follow reasonable procedures to ensure maximum possible accuracy of consumer information. Further, if a request for a consumer report included an address for the consumer that was different than the address in the file, the agency would have to notify the requestor, and credit card issuers would have to verify a change of address before issuing a new card. An identity thief often substitutes his or her home address for that of the victim, which means that new credit cards would be sent directly to the thief. Further, receipts could not include more than the last four digits of a credit card or debit card

account. These simple measures would go a long way toward protecting consumers and would not place an unreasonable burden on companies.

Identity theft and law enforcement guidelines. The bill would protect victims of identity crimes and give relief to those Texans who have lost valuable years of their lives and large sums of money trying to regain their credit ratings and their lives. Victims would be entitled to a court order declaring them to be victims of identity theft, which they could provide to employers who requested a criminal background check, creditors or credit bureaus with which they were in a dispute, or in a worst case scenario, police officers who arrested them because thieves had committed crimes in their names. The bill would simplify the process for obtaining a declaration of identity theft, which a victim could carry as a safeguard against further victimization.

The bill would ensure that law enforcement took identity theft seriously and would give them the tools to investigate it effectively. It often is impossible to interest a law enforcement agency in an identity theft crime because it is the bank or business that takes the direct financial loss, yet individual victims report it. It also is assigned low priority because it is not considered a violent crime. Furthermore, a lack of resources, guidance, and authority often prevent law enforcement from investigating all cases of identity theft. Departments typically lack an adequate number of available investigators. The bill would require DPS to create an identity theft unit to assist local law enforcement with investigations of identity theft and would require peace officers to complete education and training in identity theft.

The bill would require a peace officer to make a police report of an allegation of identity theft, regardless of where it occurred, and would give victims access to those reports, which they do not enjoy under current law. Access to a police report is important because credit bureaus will not believe a victim's story without a police report, yet peace officers often will not make a report if the crime occurred outside of their jurisdiction. Finally, the bill would ensure that victims of identity theft had certain rights guaranteed to victims of violent crime, such as the right to be informed of relevant court proceedings.

Furthermore, identity theft often crosses jurisdictional boundaries, making prosecutors unsure of where the thief should be prosecuted. These crimes

often are committed in multiple counties and could be prosecuted in any of them. The bill would allow prosecutors to indict the case in the victim's place of residence. It would be simpler and cheaper to consolidate all cases in the victim's county of residence, rather than requiring the state to bring charges and conduct trials in several counties. Furthermore, prosecuting the case in the victim's home county would locate the proceedings in the place where the most motivation exists to make the victim whole. Finally, identity thieves often prey on the elderly and other people who easily are victimized, and such people sometimes are unable to travel to another county for prosecution.

The bill would permit the attorney general to pursue identity thieves and impose hefty civil fines for violations, which would complement criminal enforcement efforts and deter businesses from placing consumers in jeopardy of identity theft. The attorney general also could recover reasonable attorney's fees and court costs, as well as restitution for a victim. Furthermore, the bill appropriately would permit the attorney general to bring an action for a restraining order or injunction to prevent violations from occurring in the first place.

Confidentiality of personal information in government records. The bill would ensure that government agencies were more responsible when collecting and distributing personal information. Members of the public should feel confident that information shared with a government agency will not be used in way inconsistent with their expectations. While citizen concerns are not new, the increasing availability of electronic records on the Internet has intensified these concerns. Because citizens are required to provide government agencies with personal information for everyday purposes, such as obtaining a driver's license, the government should be required to safeguard that information. Businesses, in turn, should not be permitted to sell such information for other purposes. Consumers are unable to track how their information is used, which makes them particularly susceptible to identity theft.

Under CSSB 405, governmental entities would have to redact certain personal identification information, such as social security numbers, before disclosing public records. Furthermore, governmental entities would have to develop written privacy policies and establish procedures to ensure that they did not collect more personal information than necessary. The Records Management

Interagency Coordinating Council would be required to provide guidance to local governments in establishing state-of-the-art records management practices. The bill would authorize governmental entities to charge someone requesting a public record a reasonable fee to cover the cost of redacting personal information to defray the costs of complying with the bill.

OPPONENTS SAY:

This bill is unnecessary. Instead, better enforcement of Penal Code, sec. 32.51 and better education for consumers on how to protect themselves is needed. Consumers could protect themselves by shredding sensitive documents, obtaining regular copies of credit reports, avoiding pre-approved credit cards, and alerting the post office to hold their mail when traveling.

While the goals of the bill are worthy, the cost to the state of implementing it would be too high. According to the Legislative Budget Board, the estimated two-year net impact to general revenue related funds would be about $500,000, which is unrealistic given the state's current fiscal crisis.

Protection of consumer information. The requirement that a credit card issuer verify a change of address would be burdensome and costly and would not prevent identity theft. Only a very small percentage of identity theft occurs through address changes. Further, many people move every year, and it is not easy to get consumers to respond to inquiries. Requiring such verification actually could assist identify thieves because it would specify an 11-day time frame after which a card could be sent to the new address.

Complying with provisions prohibiting more than four numbers to be printed on a credit card receipt could be costly to comply with because new receipt machines cost about $500. Although this amount might be insignificant to large businesses, it could be a large expense for small businesses.

Identity theft and law enforcement guidelines. Allowing venue in the county where a victim resides would be inappropriate. Offenses of every type are tried in the county where they are committed because that is where most, if not all, of the evidence is preserved. Not only might the bill make identity theft cases more difficult to prove, it could increase costs if it were necessary to move evidence, both witnesses and exhibits, to another location for trial purposes.

The bill would impose a duty on businesses to protect any personal identifying information that it collected. However, the bill would not provide businesses with any guidance or standards as to what must be done to comply. It would be unfair to subject a business to high civil penalties for violating this ambiguous provision. Businesses already spend a large amount of resources protecting these kinds of data.

Making most violations of the bill a deceptive trade practice would be overly broad. To protect businesses, the bill should specify a reasonable procedure standard for each potential violation.

The absolute prohibition against accessing or using electronically readable information from a driver's license could be counterproductive. After all, that information could be used for prevention of fraud by check and other means.

Confidentiality of personal information in government records. The financial impact of the provisions regarding the confidentiality of personal information would be harsh on cities. First of all, the bill would require each municipality to establish procedures to ensure that it collected personal information only to the extent reasonably necessary to accomplish legitimate governmental purposes, and to develop a written privacy policy. Developing these policies would cost cities time and money, and cities without the resources to do so would have to subcontract with other entities. Furthermore, cities would have to redact certain personal information from public records, or establish separate systems of records for information that could or could not be disclosed, which would require resources such as computer programs and personnel. Smaller cities that technologically are less advanced might have to do so by hand.

Further, preventing cities from disclosing certain personal information could harm businesses that use this information for a wide range of legitimate purposes. Commercial providers furnish records to business clients such as law enforcement, the FBI, banks, and governmental agencies. Oftentimes, this information helps prevent identity theft. Social security numbers are critical to verifying the identity of persons involved in transactions, such as tax liens, or to identify pension beneficiaries. After all, the verification must occur quickly, and social security numbers are the only unique identifier. Restricting access to personal information is a slippery slope. While this bill would

restrict access only to social security numbers and other specific information, next session, the Legislature might restrict access to more personal information, such as addresses. Finally, a very small percentage of identity thieves actually obtain personal information from public records, so it is more a perceived, than an actual, problem.

OTHER OPPONENTS SAY:

Protection of consumer information. CSSB 405 would not go far enough. Consumer reporting agencies should be required to take simple precautions to identify consumers before releasing credit reports. They should have to match at least four separate items of identification regarding the consumer with information about the consumer in the file. It is too easy for perpetrators to gain access to credit, and this step would provide needed safeguards. After all, if a victim lost his or her wallet, a thief could obtain credit without a photo I.D. or with an incorrect address, and it is too easy to obtain personal information over the Internet or elsewhere.

Law enforcement guidelines. The bill would not go far enough to make victims of identity theft whole. Retail stores, as well as consumers, are victims of identity theft and deserving of restitution. While they are entitled to restitution in a criminal proceeding, prosecutors often are unaware of the need for it. The bill should require law enforcement to inform retail stores of criminal proceedings so that they could obtain restitution for their losses.

NOTES:

The committee substitute made many changes to the Senate engrossed version, including:

- deleting provisions that would have required a consumer reporting agency to match at least four separate items of identification about a consumer before releasing a consumer report, and provisions that would have required an agency to verify a change of address before recording it in a consumer file;
- requiring that a person have a fraudulent intent for the offense of unauthorized use or possession of personal identifying information, and deleting provisions making it a violation to possess three or more persons' personal identifying information outside the course of business;

- changing from 10 to 30 business days the time frame within which a person would have to disclose certain information regarding an alleged violation of Penal Code, sec. 32.51;
- adding provisions authorizing the attorney general to seek restitution for a person who suffered a loss due to identity theft;
- adding exemptions to the protection of governmental records, including historical documents, information collected by TDCJ or TYC, and personal information relating to a motor vehicle accident;
- specifying that provisions regarding the privacy of governmental records would not affect the ability of a private investigator to conduct a lawful investigation;
- deleting driver's licenses from the list of personal information required to be kept private by governmental entities;
- deleting provisions permitting the release of personal information for compelling governmental interests or extraordinary circumstances, and adding exemptions to the prohibition against disclosure;
- authorized a governmental entity to charge the requestor a reasonable fee to cover the cost of redacting the information; and
- adding provisions to the Property Code protecting social security numbers and driver's license numbers in real property records.

A related bill, SB 473 by Ellis, passed the Senate on March 26 by voice vote and finally passed the House on May 25**.** It would require consumer reporting agencies to place a security alert, or a security freeze, on a consumer's file upon request by a consumer, and would prevent persons from making social security numbers available to the public.

Another related bill, HB 254 by Kolkhorst, passed the House on April 2 and was reported favorably from the Senate Criminal Justice Committee on May 21. It would allow an offense under Penal Code, sec. 32.51, to be prosecuted either in the county where the offense occurred or in a county where the victim resides.

Another related bill, SB 235 by Fraser, passed the House on May 16 and was sent to the governor. It would require sellers to print no more than the last

four digits of a credit card account number on a receipt, and would provide a civil penalty of up to $500 for each month a which a violation occurred.