HOUSE
RESEARCH
ORGANIZATION
Texas House of Representatives

focus REPORT

September 27, 2004

Combatting Identity Theft

The Texas Legislature and the U.S. Congress recently enacted laws to combat the crime of identity theft. These laws, and proposals for additional changes, generally are designed to reduce incidents of identity theft, to better and more quickly identify cases when they occur, and to facilitate their investigation and prosecution. Interest in preventing identity theft has grown as the number of victims and the seriousness of the crime have increased and as the costs to victims and businesses in time and money have risen. In addition, concerns about homeland security have placed a higher priority on preventing identity theft that could facilitate terrorist activities.

Most laws dealing with identity theft focus on three areas: criminal penalties for certain offenses, requirements for the credit industry to include certain information in credit reports or to restrict access to credit and credit reports, and the privacy of personal data. In Texas, laws enacted by the 78th Legislature in 2003 focused on requiring credit agencies to issue security alerts and freezes, expanding the venues where identity theft can be prosecuted, and restricting the display of Social Security numbers and credit card numbers. In December 2003, Congress enacted a law dealing with credit transactions. The new federal law has provisions similar to some enacted by the 78th Legislature and may preempt parts of the Texas law where the two conflict. In July 2004, the federal government again added to its identity theft laws by requiring additional and longer prison sentences when identity theft is committed in connection with certain other federal crimes.

This report examines current law and new proposals designed to reduce incidents of identity theft, to better and more quickly identify cases when they occur, and to facilitate their investigation and prosecution.

Background on identity theft

Identity theft occurs when someone uses another's personal identifying information without permission to commit crimes such as fraud or theft. Thieves can use personal information such as Social Security numbers, driver's license numbers, names, addresses, birth dates, financial records, or financial institution PIN numbers to use existing credit cards, obtain new credit cards, make purchases, or take over financial accounts. Another form

One victim's experience

One woman's testimony before a House State Affairs Committee hearing on August 9, 2004, illustrates the toll that identity theft can take on the lives of victims. This witness testified that a hotel maid stole her personal information and used it to commit numerous frauds, including reopening credit card accounts that had been inactive for more than 20 years and attempting to establish new identities using her Social Security number, a practice commonly known as "cloning." The witness said that she remains traumatized three years after these crimes occurred and that she has spent some $50,000 in restoring her identity. She testified that the identity theft also made it difficult for her to qualify to work as a volunteer with her daughter's Brownie troop because she was unwilling to reveal her Social Security number for a background check.

of identity theft, known as "criminal" identity theft, is committed when a thief gives law enforcement officers another's name or other identifying information during a police investigation or arrest.

Identity thieves use a variety of methods to obtain another's personal information, including stealing credit card numbers, eavesdropping on conversations, looking through a victim's records or statements in the trash, calling a victim and pretending to be a bank or other organization, and hacking into computer files.

Estimates of the number of victims of identity theft vary. In a Federal Trade Commission (FTC) survey conducted in early 2003, 4.6 percent of those surveyed said they had been victims of some type of identity theft in the past year, which translates into almost 10 million victims for 2002. The survey estimated that these cases of identity theft amounted to about $5 billion in losses to individuals and $48 billion in losses for businesses and financial institutions. The survey also reported that 12.7 percent of respondents said that they had been victims of identity theft over the previous five years, which translates into about 27 million victims over that period. The study is available online by clicking here.

The FTC also reported that in 2003 it received approximately 215,000 reports of identity theft, up from almost 162,000 in 2002. The FTC received reports of about 21,000 identity theft victims in Texas, which translates into 93.3 victims per 100,000 population, the fourth highest ranking among states. Arizona had the highest rate with 122.4 victims per 100,000, and South Dakota's rate of 19.6 per 100,000 was the lowest.

Many of the proposals to change Texas law concerning identity theft involve criminal statutes. These proposals include instituting a presumption to harm or defraud under certain circumstances in which a person possesses another's identifying information, creating a new offense for possessing or making fake identification cards, increasing penalties for providing false information to peace officers and criminal use of scanning devices, expanding the venues for prosecuting some identity theft crimes, expanding the ability of courts to order restitution for certain identity theft crimes, and deleting some specific Transportation Code offenses dealing with fraud in driver's licenses and identity cards.

Current law

Current law addresses identity theft by establishing criminal penalties for specific offenses, requiring certain notifications about potential identity theft, restricting access to consumers' credit and credit reports and to individuals' private information, and requiring the state's Department of Public Safety (DPS) to investigate identity theft and associated crimes.

Criminal offenses. While numerous criminal statutes can be used to prosecute identity theft, one deals specifically with the crime. Penal Code sec. 32.51 makes the fraudulent use or possession of identifying information a criminal offense. It is a state-jail felony (see *Criminal penalties associated with identity theft*, right) to obtain, possess, transfer, or use another person's identifying information without that person's consent and with intent to harm or defraud another. The 78th Legislature, through HB 254 by Kolkhorst, allowed this offense to be prosecuted either in the county where the offense occurred or in the county where the victim lives.

Other statutes that relate to identity theft include:

- Penal Code sec. 32.32, which makes it an offense to intentionally or knowingly make a false or misleading statement to obtain property

or credit. Punishment can range from a class C misdemeanor to a first-degree felony depending on the value of the property or amount of credit;

- Penal Code sec. 32.31, which lists numerous state-jail felonies involving credit card or debit card abuse, including presenting or using a credit card or debit card with the intent to obtain a benefit fraudulently and with the knowledge that the card is being used without the consent of the cardholder;

- Penal Code 37.10, which deals with giving false information for government records and can be used when false information is provided for a driver's license or state identity card;

- Numerous Transportation Code violations found in chapter 521 that deal with false information on driver's licenses, illegal use of licenses, and counterfeit licenses; and

- Business and Commerce Code sec. 35.58, which makes it a class B misdemeanor to use 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 authorized user's consent and with intent to harm or defraud. This section was added by the 78th Legislature through HB 2138 by Hopson.

Federal law also makes identity theft a crime. In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act (18 USC 1028), making it a federal crime to knowingly use another person's identification with the intent to commit a federal crime or a state felony. The law also required the FTC to establish a clearinghouse for statistics and information about identity theft. In practice, violations of state laws rarely are prosecuted under this federal statute.

In July 2004, Congress enacted the Identity Theft Penalty Enhancement Act (ITPEA), creating the offense of aggravated identity theft. This new offense is defined as the unauthorized transfer, possession, or use of another's identification during the commission of other specified federal felonies. The law requires that prison terms of two or five years be added to the sentence given for the related felony.

Criminal penalties associated with identity theft

The following penalties are associated with identity theft and similar crimes under various Texas statutes.

- **First-degree felony** – life in prison or a sentence of five to 99 years and an optional fine of up to $10,000.
- **Second-degree felony** – two to 20 years in prison and an optional fine of up to $10,000.
- **Third-degree felony** – two to 10 years in prison and an optional fine of up to $10,000.
- **State-jail felony** – 180 days to two years in a state jail and an optional fine of up to $10,000.
- **Class A misdemeanor** – up to one year in jail and/or a maximum fine of $4,000.
- **Class B misdemeanor** – up to 180 days in jail and/or a maximum fine of $2,000.
- **Class C misdemeanor** – maximum fine of $500.

State and federal restrictions on credit reports. The 78th Legislature in 2003 enacted a law giving consumers the right to request a security alert or security freeze on their files held by consumer reporting agencies. A security alert notifies the recipient of a consumer report that the consumer's identity may have been used fraudulently to obtain goods or services. A security freeze prohibits a consumer reporting agency from releasing a report relating to the extension of credit involving that consumer without the consumer's authorization.

Under SB 473 by Ellis, a consumer reporting agency must place a security alert on a consumer's file within 24 hours of receiving the consumer's request, and the alert must remain in effect for at least 45 days. A person who receives notification of a security alert in connection with a request for a consumer report for the approval of a credit-based application or for an application for a non-credit-related service may not lend money, extend credit, or authorize an application without taking reasonable steps to verify the consumer's identity.

Laws and proposals to prevent theft of Social Security numbers

Many cases of identity theft center on the use of another's Social Security number (SSN) because financial institutions, insurance companies, government offices, and businesses commonly use SSNs to identify individuals.

The 78th Legislature in 2003 enacted a law, effective January 1, 2005, that restricts the distribution or display of SSNs. SB 473 by Ellis et al., generally prohibits a person, other than an governmental entity from:

- intentionally communicating or making someone's SSN available to the general public;
- displaying a person's SSN on a card or other device required to access a product or service;
- requiring a person to transmit a SSN over the Internet, unless the connection is secure or the number is encrypted;
- requiring a person's SSN for access to a website, unless a password or other authentication device also is required; or
- printing a person's SSN on any materials, other than a form or application, sent by mail, unless required by state or federal law.

Part of the debate surrounding legal restrictions on the use of SSNs focuses on whether similar restrictions should apply to government. The 78th Legislature enacted a number of laws dealing with restrictions on the governmental disclosure of SSNs, including:

- HB 500 by Goolsby, which prohibits public disclosure of certain personal information, including SSNs, of disabled or elderly persons who request a tax exemption;

- HB 1863 by Bohac, which makes SSNs and certain other personal information furnished on voter registration applications confidential information that is not considered public information under the state's Open Records laws;

- HB 1027 by Hupp, which allows government employees who also are crime victims as defined by the Crime Victims Compensation laws to decide whether to allow public access to their identifying information held by the Attorney General's Office's or other governmental bodies; and

Upon a request that includes a copy of a valid police report or criminal complaint of identity theft, an agency must place a security freeze on a consumer's file within five business days. Within 10 days, the agency must send confirmation to the consumer, along with a unique identification number or password that the consumer may use to authorize removal or temporary lifting of the freeze. Security freezes and alerts do not apply to certain companies, including check service companies, and security freezes do not apply to a consumer report provided to a state or local governmental entity acting under a court order, warrant, or subpoena.

Questions have arisen about whether it is appropriate to require that victims obtain a valid police report or complaint in order to have a security freeze placed on their files. While some argue that this requirement is necessary to ensure that freezes are used in appropriate situations, others argue that all consumers should have the option of freezing their files and that the option may be especially appropriate for certain Texans, such as nursing home residents.

Under SB 473, the attorney general may file suit for injunctive relief to prevent a violation of the security alert and freeze provisions or for a civil penalty not to exceed

- HB 2930 by Lewis, which prohibits county clerks from rejecting certain documents relating to transfers of property because the instruments do not contain SSNs and requires that notice be given that the documents do not have to contain SSNs.

Other bills dealing with the privacy of SSNs failed to pass during the 2003 regular session. HB 1015 by Miller, et al., which was approved by the State Affairs Committee but died in Calendars, would have prohibited a governmental body from disclosing to the public as part of an Open Records request a person's SSN without permission. An exception would have exempted local governments from the prohibition if the number existed in information created before September 1, 2003.

SB 405 by Hinojosa, which died in the House, would have prevented state and local governmental entities from disclosing certain personal information, including SSNs, to the public and would have required them to redact or obscure the personal information from documents available to the public. Governmental entities would have been able to charge a reasonable fee to persons requesting the information to cover the costs of redacting it. Also, the bill would have required governmental entities to establish procedures to ensure that they collected personal information only to the extent reasonably necessary to accomplish a legitimate government purpose, and local and state governments would have had to develop written privacy policies.

In general, supporters of restricting governmental disclosure of SSNs say that it would ensure that government agencies were more responsible when collecting and distributing personal information that citizens must provide for everyday purposes. Restrictions on information also could help curb the use of personal identifying information such as SSNs and prompt government offices to come up with other ways to identify persons, thus reducing opportunities for identity thieves to obtain information for criminal purposes.

Opponents of the proposals say that while these goals may be worthy, the costs of implementation would be too high. The financial burdens placed on cities and counties by these restrictions would be especially onerous, they say. Developing privacy policies, establishing procedures to limit the collection of personal information, redacting public records, or creating separate systems of records for information that could or could not be disclosed would require additional resources such as computer programs and personnel. Also, opponents say, preventing governments from disclosing personal information could harm businesses that use this information for a wide range of legitimate purposes and that adequately safeguard it.

$2,000 per violation. The state Office of Consumer Credit Commissioner is required to report to the legislative leadership by December 31, 2004, as to whether provisions of SB 473 should remain in effect after September 1, 2005.

A recent federal law that deals with credit transactions may preempt part of SB 473. The Fair and Accurate Credit Transactions Act (Public Law No. 108-159 (2003)) (FACTA), enacted in December 2003, establishes a nationwide system of fraud alerts. It requires nationwide credit reporting agencies to include a fraud alert in a consumer's files for at least 90 days if requested by the consumer and requires the agencies to include an extended fraud report in the consumer's files for up to seven years if the consumer files an identity theft report or a federally developed affidavit of identity theft. Fraud alerts require credit reports to indicate that the consumer may have been a victim of identity theft and tell the user of the report that the consumer does not authorize any granting of credit or additional credit cards unless the report user verifies the identity of the person making the request. According to Texas' Office of Consumer Credit Commissioner, its December 2004 report to the legislative leadership should include an analysis of which, if any, potentially conflicting state

provisions dealing with identity theft are preempted by the federal law.

The federal law also requires credit reporting agencies to provide one free credit report each year to consumers who request them and to give additional free copies of their files to consumers while the files contain fraud alerts. These provisions apply to the states according to staggered deadlines and will be available to Texas consumers beginning June 1, 2005.

Printing credit card numbers on receipts. Both state and federal law restrict the printing of credit card numbers on receipts, but the two provisions may be in conflict. In SB 235 by Fraser, the 78th Legislature prohibited the printing of more than the last four digits of a credit or debit card account number or the month and year of the card's expiration date on a receipt for a transaction and made violators of the new restrictions civilly liable to consumers. Violators of this prohibition are liable to the state for a civil penalty of up to $500 for each month a violation occurs, but the penalty cannot be imposed for more than one violation per month.

FACTA, enacted after the new Texas law, requires that no more than the last *five* digits of credit and debit card numbers be printed on a receipt. As with other provisions in FACTA, some analysts believe that federal law may preempt state law in this case.

Law enforcement. A proposal that was not enacted during the 78th Legislature would have required peace officers who received a report of identity theft to make a written report and provide the victim with a copy. Some identification theft victims report problems obtaining police reports from law enforcement. Without these reports, it can be difficult for victims to convince creditors that they should not be held responsible for unauthorized purchases. Others point out that decisions about when to generate police reports are best left to the discretion of officers who can determine the merits of each case. The FTC has developed an identity theft affidavit that can be used by victims for reporting their cases to creditors, which is available online by clicking here.

Another proposal that was not enacted by the 78th Legislature would have required the DPS director to create an identity theft unit to help local law enforcement agencies investigate identity theft. However, the Legislature did authorize DPS to create a Driver License Division Fraud Unit that, according to DPS, is working with federal and local law enforcement offices to investigate cases involving identity theft, sale of personal information, counterfeiting government documents, and tampering with governmental records as they relate to driver's licenses. In testimony before the Senate Criminal Justice Committee in August 2004, DPS recommended that the 17-person unit receive additional manpower to address the growth in identity fraud and theft.

DPS also said that it will seek approval during the 79th Legislature to incorporate image verification technology into its re-engineered driver's license system. This technology, according to DPS, would allow the department to compare photographs in its database of license and identification card holders to identify persons holding multiple records and to verify an applicant's identity when issuing a license.

In addition, some Texas financial institutions and law enforcement agencies, including DPS, are cooperating through the Loss Avoidance Alert System to alert each other about potentially illegal actions, including identity theft. For example, if one organization learned of an identity thief passing forged checks, that organization could alert members of the system via e-mail to watch for checks that originate from the stolen account.

Proposals to change criminal laws

Prosecuting identity theft without intent to harm or defraud. Under Penal Code sec. 32.51, the Texas statute that deals most directly with identity theft, a person must possess or use another's identifying information with intent to harm or defraud another. Some law enforcement officers say that it can be difficult to prove the intent of a thief who possesses stolen identity documents but has not yet used them. One proposed solution would institute a presumption of harm or fraud if the accused thief possessed the identity of more than one other person.

According to supporters, this proposal would allow prosecutors more easily to bring cases against identity thieves who were caught before they used stolen information and would be similar to the presumption in Penal Code sec. 37.10, which involves tampering with a government record. In the tampering section, the offense

is a second-degree felony if there was intent to defraud or harm another, and there is a *presumption* of intent to defraud or harm another if the person has two or more of the same type of specified governmental records or forms. Supporters say the same presumption of intent should apply to suspects caught possessing the identifying information of multiple persons. The proposal, however, would continue to require prosecutors to prove intent to harm or defraud in a case, such as a juvenile carrying a fake ID, where someone might illegally possess another's identity without the intent to commit fraud or theft.

Opponents of the proposal argue that the burden of proving intent to harm or defraud should remain on the state, where it has been rightfully placed, and that it should remain the state's duty to prove elements of an offense beyond a reasonable doubt as required by the U.S. and state constitutions. If an accused identity thief possesses identifying documents of numerous persons, the state should not have trouble proving intent to harm or defraud, they say.

Higher penalty for providing law enforcement with another's identification. Penal Code sec. 38.02 currently makes it a class B misdemeanor for a person to intentionally give a false or fictitious name, address, or date of birth to a peace officer who has lawfully arrested or detained the person. One proposal would make it a class A misdemeanor or a state-jail felony to provide the identifying information of another person to a peace officer. Providing a real person's name to a peace officer is a more serious crime than giving a fictitious name, proponents say, because it creates a real victim whose name could end up in the criminal justice system and who could become the subject of an arrest warrant.

Opponents of the proposal say that the Legislature should not inflate the penalties for crimes, such as those under sec. 38.02, that are more appropriately punished with a lesser penalty. The harm done by violating sec. 38.02 is in obstructing justice by lying to a peace officer, they say, not in the nature of the false name given. If someone gave a police officer a false name that turned out to be the name of a real person, it could be difficult to determine if the offender intended for the name to be fictitious or planned to assume the real person's identity, opponents say.

New offense for possessing or making fake government ID. "Novelty" identification cards that carry the name of a state, nation, or government agency currently can be purchased through the Internet or at flea markets and often are used by identity thieves. Although many cards look like authentic Texas-issued driver's licenses or identity cards, sellers of the cards make them legal by stamping them with the words "not a government document." However, these words often can be removed easily, making it difficult to distinguish a fake ID from an authentic identity card.

One proposal would make it illegal to possess or make a document carrying the name of a state, nation, or governmental agency that reasonably could be perceived as a legitimate form of identification. Supporters say that prohibiting the use of governmental names on any "identity" card not actually issued by the government could reduce the value of these fake IDs to identity thieves since most retailers will accept only identification that displays a governmental name. Critics of the idea say the new offense would be unlikely to deter identity thieves who are intent on using the cards to commit other lucrative crimes.

Higher penalty for illegal use of scanning devices. DPS recommended in its August 24 testimony before the Senate Criminal Justice Committee that the penalty in Business and Commerce Code, sec. 35.58 for using a scanning device or re-encoder to obtain information from a credit or debit card be increased from a class B misdemeanor to a third-degree felony if the information is used for identity theft or any other criminal purpose. Supporters say that these tougher punishments would be more appropriate for the serious crime of identity theft. Opponents argue that it would be improper to punish this activity in the same manner as serious, violent crimes by instituting a felony that can carry a prison term. Changing the offense to a third-degree felony also would skip over the state jail felony, which was designed to punish less serious property crimes, such as the illegal use of a scanning device.

Expand venue for prosecution of false statement to obtain credit. Prosecutions for making a false or misleading statement to obtain property or credit under Penal Code sec. 32.32 must be made in the county in which the offense occurred. A proposed change would expand the venue where this offense can be prosecuted to include the county where the victim lives. This would give prosecutors the same option when going after identity thieves under sec. 32.32 as the 78th Legislature gave them for prosecuting the crime of fraudulent use or possession of identifying information.

Supporters say that some serious identity theft cases are best prosecuted under sec. 32.32 because the punishment can be as severe as a first-degree felony, which might encourage prosecutors to pursue such cases more aggressively. Identity theft crimes, including those under sec. 32.32, often are committed in multiple counties and could be prosecuted in any of them. In these cases, it might be simpler and cheaper to consolidate them in the victim's county of residence, which further could motivate prosecutors to pursue cases because victims would be close by. With the resources available today, relocating a case to a victim's county should not present any problems, supporters say.

Critics of the idea say that offenses of every type are tried in the county where they are committed because this is where most, if not all, of the evidence exists. Allowing certain cases to be prosecuted elsewhere could make them more difficult to prove and increase costs if witnesses and exhibits had to be moved.

Delete offenses in Transportation Code. DPS recommended in its testimony before the Senate Criminal Justice Committee that specific offenses in Transportation Code chapter 521, subchapter S, that deal with fraud in applications for Texas driver's licenses or identification cards be deleted, allowing prosecutors to bring these cases under Penal Code sec. 37.10, which involves tampering with governmental records. The Penal Code provisions are broader, according to DPS, and therefore should be easier for prosecutors to use. Penalties for tampering with governmental records range from a class A misdemeanor to a second-degree felony, depending on the circumstances of the crime. Critics of the proposal say that the specific crimes in the Transportation Code were created to handle specific situations that still exist.

Expand the ability of courts to order restitution for certain identity theft crimes. Another proposal would include the Penal Code sec. 32.32 offense of making false statements to obtain credit among the list of identity theft offenses for which courts specifically may order convicted defendants to make restitution to their victims. Courts currently have this authority for defendants convicted of the general identity theft offense of fraudulent use or possession of identifying information found in Penal Code sec. 32.51. Supporters of this idea argue that since some of the most serious cases that cause victims the most harm are prosecuted under sec. 32.32, courts should have restitution authority in that section as well. Critics say that the Legislature should not create any additional special circumstances that are exceptions to the general laws under which offenders already may be ordered to pay restitution.

— by Kellie Dworaczyk

HOUSE RESEARCH ORGANIZATION

Steering Committee:

Roberto Gutierrez, *Chairman*
Dianne White Delisi, *Vice Chairman*
Harold Dutton
Peggy Hamric
Bob Hunter
Carl Isett
Mike Krusee
Jim McReynolds
Geanie Morrison
Elliott Naishtat
Joe Pickett
Robert Puente
Elvira Reyna
G.E. "Buddy" West
Steve Wolens

John H. Reagan
Building
Room 420
P.O. Box 2910
Austin, Texas 78768-2910

(512) 463-0752
FAX (512) 463-1962

www.capitol.state.tx.us/hrofr/hrofr.htm

Staff:

Tom Whatley, *Director;* Ben Davis, *Editor;*
Rita Barr, *Office Manager/Analyst;* Betsy Blair,
Kellie Dworaczyk, Patrick K. Graves,
Tedd Holladay, Kelli Soika, *Research Analysts*