LEGISLATIVE REPORT

REVIEWING IDENTITY THEFT AND SENATE BILL 473

REPORT PREPARED BY
THE OFFICE OF CONSUMER CREDIT COMMISSIONER
SUBMITTED: DECEMBER 30, 2004

IDENTITY THEFT

Executive Summary

During its 78th Session, the Texas Legislature passed Senate Bill (SB) 473. This legislation is a state effort clearly designed to help reign in identity theft in Texas, to protect Texans from identity thieves, and to give Texans tools to utilize in the event of victimization. Senate Bill 473 includes a provision that requires the Office of Consumer Credit Commissioner (OCCC) to review the impact and efficacy of that Act and to make a recommendation to the Lieutenant Governor and the Speaker of the House of Representatives not later than December 31, 2004 as to whether the Acts' provisions should remain in effect after September 1, 2005.

SCOPE OF THE PROBLEM

- The Federal Bureau of Investigation has now acknowledged identity theft as one of the country's fastest growing crimes
- Of all states, Texas ranked 4th highest in number of complaints filed to the FTC per 100,000 citizens.
- 93.3 of every 100,000 Texans reported complaints to the FTC.
- It cost businesses about $48 billion to repair the damage inflicted by ID theft.
- It cost consumers about $5 billion to repair the damage inflicted by ID theft

GOVERNMENT TAKES ACTION

- During its 78th Session, the Texas Legislature passed Senate Bill (SB) 473. The bill's stated purpose involves, "assisting consumers to prevent and detect identity theft; providing penalties."
    - This legislation is a state effort clearly designed to help reign in identity theft in Texas, to protect Texans from identity thieves, and to give Texans tools to utilize in the event of victimization.
- Subsequent to the passage of SB 473 in Texas, the United States Congress passed the Fair and Accurate Credit Transactions Act (FACT Act). The FACT Act, signed into law on December 4, 2003, actually amends the federal Fair Credit Reporting Act (FCRA).
    - The FTC stated that the FACT Act, "will help reduce identity theft and help victims recover."

FEDERAL PREEMPTION ANALYSIS

- Generally, Texas can enact statutes that relate to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, to the extent that those statutes are not inconsistent with any provision of the federal FCRA.
- The United States Congress has enacted certain provisions of the federal FCRA that cannot be altered, affected, annulled, or changed by state law.
- These provisions are set forth under the federal FCRA, 15 U.S.C.A. Section 1681t. There are three recognized forms of federal preemption, each of which is unique:
    - (1) subject matter preemption;
    - (2) disclosure-related preemption; and
    - (3) conduct preemption.

CONCLUSION

In analyzing the identity theft provisions of SB 473, it becomes apparent that many issues addressed by SB 473 are also addressed by the FACT Act. In many cases, the FACT Act identity theft provisions preempt state identity theft law and render those affected provisions of SB 473 substantially less effective, if not completely ineffective.

There are two notable exceptions where consideration of continuation of state law provisions should be observed. The provisions contained in Section 5 of SB 473 pertaining to enforcement actions with respect to

other violations of Chapter 20, Business and Commerce Code, is one of those cases. Section 6 governing control of social security numbers as it applies to non-consumer reporting agencies also offers opportunity for continued state regulation.

The rapid growth of identity theft crime signifies it as both a continuing and critical issue with which to deal. The Legislature is wise to continue reviewing information related to the crime and taking action when it is required.

IDENTITY THEFT

"More than ever, the information explosion, aided by an era of easy credit, has led to the expansion of a crime that feeds on the inability of consumers to control who has access to sensitive information and how it is safeguarded. That crime is identity theft."[1]

Recognizing the seriousness of the rapid and continuing growth of identity theft crimes, governments have started taking action, requiring businesses to take steps to secure consumer information and granting consumers new power to protect their credit and restore that credit when it is ransacked by an identity thief.

During its 78th Session, the Texas Legislature passed Senate Bill (SB) 473. This legislation is a state effort clearly designed to help reign in identity theft in Texas, to protect Texans from identity thieves, and to give Texans tools to utilize in the event of victimization. The Governor signed the bill on June 22, 2003, and the bill became law on September 1, 2003.

Senate Bill 473 includes a provision that requires the Office of Consumer Credit Commissioner (OCCC) to review the impact and efficacy of that Act and to make a recommendation to the Lieutenant Governor and the Speaker of the House of Representatives not later than December 31, 2004 as to whether the Acts' provisions should remain in effect after September 1, 2005. This report is the result of the OCCC's review.

SECTION I: SCOPE OF THE PROBLEM

Signaling recognition of the growing problem of identity theft, the Federal Trade Commission (FTC) began collecting identify theft complaints from consumers on November 1, 1999. Every year since, the FTC has seen the number of related complaints that it fields increase.[2] To gain a clearer and more complete understanding of the scope of the identity theft problem than complainant data alone could reveal, the FTC commissioned a private firm to conduct a nationwide study in March and April 2003. After reviewing the data collected, Betsy Broder, Assistant Director of the Division of Planning and Information, Bureau of Consumer Protection, FTC, said, "Identity theft is more widespread and pernicious than previously realized."[3] In fact, the Federal Bureau of Investigation has now acknowledged identity theft as one of the country's fastest growing crimes.[4]

As more people use the Internet for services like banking, the sensitive nature of the information being shared online raises general concerns in the minds of citizens about the privacy of their personal information—encompassing both what happens to information in digital transit and what companies and other organizations do with that data once it is collected—and the security of their financial records. Businesses and government organizations share the public's concerns. While identity theft and fraud existed before the culture's rapid embrace of the Internet, never before have the perpetrators of those crimes had it so easy or been so successful.

IDENTITY THEFT FACTS AND STATISTICS

- The Department of Justice reports that ID theft is the nation's fastest growing financial crime.[5]
- In 2003, 3.2 million consumers had new accounts opened or other fraud committed in their names.[6]
- In 2003, 6.7 million consumers experienced misuse of an existing account.[7]
- in 2003, of the almost 10 million American victims of identity theft, 500,000 were children. Children often do not find out they have been the victims of fraud until years later, when they apply for student loans or other credit for the first time.[8]
- It cost businesses about $48 billion to repair the damage inflicted by ID theft.[9]
- It cost consumers about $5 billion to repair the damage inflicted by ID theft.[10]
- In 2003, nearly 10 million Americans discovered they were victims of some form of identity theft.[11]
- Victims of identity theft in 2003 spent a total of almost 300 million hours to correct the problems caused by the theft.[12]

- It normally takes victims of ID theft 2 years to clear up problems related to the theft.[13]
- Of fraud complaints to the FTC in 2003, 58% of those activities were initiated online, 18% by phone, and 13% by mail.[14]
- 42% of all complaints to the FTC in 2003 related to ID theft.[15]
- Internet related fraud accounted for 55% of all fraud reported to the FTC in 2003.[16]
- Of all ID theft reports to the FTC in 2003, 50% involved credit card or bank fraud.[17]
- Of the 50 states, Texas ranked 4th for the highest number of complaints filed per 100,000 citizens.[18] 93.3 of every 100,000 Texans reported complaints.[19]
- In Texas, 49% of all identify theft cases reported to the FTC in 2003 involved credit card or bank fraud.[20]
- During 2003, 20,634 Texans reported identity theft complaints to the FTC.[21]

How Do Criminals Use Electronic Methods to Steal Someone's Identity?

Identity thieves really only need three pieces of information to open credit card or bank accounts in another's name: a full name, a social security number, and a date of birth.[22]

There are a number of common schemes that criminals utilize to steal a person's identity. Many of the tactics involve electronic mechanisms that facilitate information heists, while others employ more rudimentary tools.

- Stealing company data. Millions of identities can be stolen in a single attack by hackers or company insiders in assaults on company databases or commercial Web sites where credit card or other personal information is stored.[23]

- Pretexting. This occurs when someone uses a false pretense to lure a victim into revealing personal information. An example: a consumer responds to an apparently legitimate e-mail from a business requesting personal information to update company records. When the consumer replies with the requested information, it actually goes directly to an ID thief who then has all the information they need to steal the unsuspecting consumer's identity.[24]

    - Phishing. This is a variant of pretexting. In this scam, criminal groups create a Web site that masquerades as the home page of an Internet provider, financial institution, or other business. The perpetrators then send out e-mails directing potential victims to the fake site. Once on the site, the potential victims are asked to update personal information for company records. It should be noted that these fake Web sites are very well done.[25]

- Spyware. This is a form of software that is frequently imbedded in pop-up ads and Internet e-mail attachments. Legitimate advertisers use the technology to tailor content to an individual's tastes; however, spyware can also be used by unknown perpetrators to raid a user's hard drive.[26]

- Skimming. Criminals use handheld magnetic card readers to retrieve personal information from the magnetic strip on credit and debit cards. Automatic teller machines have also been rigged by criminals to record information from magnetic strips.[27]

- Old Computers. It is relatively easy to raid the hard drives of discarded computers for personal information.[28]

Although this list includes the common schemes, the most imaginative identity theft plots defy simple categorization. In 2000, two men perpetrated, with very little effort, the largest single identity theft scheme in history. Philip Cummings, a thirty-two year old English immigrant, worked at a telephone help-desk job at

Teledata Communications. The small company where Cummings worked made credit prompter boxes, simple credit check terminals that are used at more than 25,000 businesses across the United States. As one of the hundreds of third-party service providers, Teledata had access to credit report data at all the major credit bureaus. Cummings and his partner, Linus Baptiste, also had access to that data by virtue of Cummings job with Teledata.

By using codes that Cummings had access to at his job, Cummings was able to gather credit reporting information by impersonating almost any company authorized to obtain credit reports from the credit bureaus. The credit reports the codes provided would allow the perpetrators to commit identity theft on just about anyone in the American credit system. Splitting $60 a report, Cummings and Baptiste stole thousands of credit reports that Baptiste told Cummings he was passing along to Nigerian partners. Cummings was not even at Teledata very long, but when he left, he took a spreadsheet of user names and passwords that allowed him continued access to credit reports at all three credit bureaus.

The criminals were selective in the credit reports that they stole too. They picked out people at addresses in wealthy neighborhoods across the country. They were able to pilfer credit reports for 10 months before anyone even noticed. By the time the criminals were finally captured, there was no way to estimate either the millions of dollars in losses to consumers and business or the time spent to clean up the mess. In the end, at least 33,000 consumers were victimized by the scheme and had untold consumer goods and loans obtained in their names.[29]

NOT ALL THE BEST METHODS ARE ELECTRONIC

Although the American consumer's rapid embrace of technology and increasing use of the Internet have augmented the tools available to the identity thief, these crooks have certainly not abandoned their more traditional methods of stealing. Identity thieves still commonly use just a phone and their own charisma to gain access to the vast amounts of personal, non-public information that companies routinely maintain.

Consider the case of James Rinaldo Jackson: A big fan of Steven Spielberg, Mr. Jackson's strong fascination led him to monitor everything that Mr. Spielberg charged on his American Express credit account for an entire year. How? *While in a federal prison*, Mr. Jackson managed to secure all kinds of personal, non-public information about the famous film director, as well as about 100 other folks in Hollywood, with just a few phone calls.

To get Spielberg's data, Jackson called the Screen Actor's Guild and conned an operator into supplying him with the name of the guild's insurance provider. Jackson then called the insurance provider and, acting as an administrator at a medical provider trying to confirm coverage for billing purposes, tricked operators into supplying him with social security numbers, dates of birth, addresses, etc. Finally, Mr. Jackson phoned American Express, identifying himself as Steven Spielberg. When the American Express operator asked him if he was *the* Steven Spielberg, Mr. Jackson replied that he was not, but that people mistook him for the famous director all the time. After establishing a rapport with the American Express phone operator, Mr. Jackson proceeded with his plan to access the real Spielberg's accounts. The operator asked for an account number, but Jackson replied that he'd accidentally left his card at home. The operator then asked for a social security number and date of birth, which Jackson could of course provide due to his earlier research on Spielberg. From there, the operator gave Mr. Jackson all the details of the real Spielberg's account, including: the balance on the account, a comprehensive breakdown of the billing, the amount of the last payment, and the amount due. Jackson learned where Spielberg ate, where he bought his clothes and shoes, and all the other details about the real Spielberg's life that a month of charges would reveal.[30]

Other identity thieves find success using as a key component of their plot a technology that predates even the phone. Letters written on fake letterhead were the primary element in Abraham Abdallah's scheme to

bilk over 200 of the individuals listed in the 2001 *Forbes 400* magazine. Abdallah gained the key information he needed by preparing fraudulent letters bearing the names of companies like Goldman Sachs and Bear Stearns, which he sent to credit bureaus requesting credit reports on his potential victims. The credit reporting companies unwittingly supplied Abdallah with the information he wanted most: the victims' social security numbers and the location of their accounts. With the new information in hand, Abdallah used a cell phone, voice mailboxes, free e-mail accounts, and fake PO boxes purchased in the names of the world's wealthiest people to access billions of dollars. Abdallah, "could call Paul Allen's [co-founder of Microsoft, current owner of the Portland Trailblazers (NBA) and Seattle Seahawks (NFL)] broker and request a transfer, leaving what appeared to be a West Coast callback number. But it was just a voice mailbox."[31]

CAN CONSUMERS PROTECT THEMSELVES?

Consumers should certainly take every legitimate step possible to protect themselves from identity thieves. Personal information should be safeguarded in homes. Personal identification numbers should not be kept near checkbooks, ATM or debit cards; papers with confidential data on them should be shredded (includes credit card offers, receipts, cancelled checks, bank statements, medical bills, insurance documents, etc.). People should not carry a social security card in their wallets or purses and should carry only the credit cards they actually need. Consumers should be wary of the entities they give their personal information to and should be aware of current electronic scams (phising, pretexting, etc) and should secure their electronic data that is stored on personal computers. Consumers should not supply any personal information to a business unless the consumer themselves initiated the contact and knows that the business is a credible one. Consumers should check their billing statements each month for unauthorized activity and should also be concerned if a bill fails to arrive on time. Consumers should not put personal information on credit card receipts and should make sure not to leave receipts behind at the store. Consumers should also be wary of any actual credit cards or any other notices of credit received in the mail for which they did not apply. In these instances, consumers should fully investigate the circumstances surrounding the credit offered.[32]

Still, even if a consumer takes every reasonable and legitimate action to secure their personal information, there is no guaranteed protection from identity thieves. Critically important, a consumer can be a victim of identity theft through no fault or oversight of their own. After all, neither Steven Spielberg nor Paul Allen bore any complicity in the acts that made them identity theft victims; they just happened to be well-known and wealthy. And the 33,000 victims of Linus Baptiste and Philip Cummings did nothing more than millions of other Americans: they participated in the American credit system, their personal information on file at the major credit bureaus. Ultimately, a consumer does not have to be either gullible or naive to be fleeced by identity thieves: An individual can take every possible precaution against identity theft, yet still find that they have been victimized.

SECTION II: GOVERNMENT TAKES ACTION

In many cases of identity theft, consumers' non-public personal information is stolen from a business or credit bureau. Clearly, consumers alone cannot protect themselves. Recognizing the seriousness of the rapidly growing crime, governments have started taking action, requiring businesses to take steps to secure consumer information and granting consumers new power to protect their credit and restore that credit when it is ransacked by an identity thief.

During its 78th Session, the Texas Legislature passed Senate Bill (SB) 473. The Governor signed the bill on June 22, 2003, and the bill became law on September 1, 2003. The bill's stated purpose involves, "assisting consumers to prevent and detect identity theft; providing penalties."

Subsequent to the passage of SB 473 in Texas, the United States Congress passed the Fair and Accurate Credit Transactions Act (FACT Act). The FACT Act, signed into law on December 4, 2003, actually amends

the federal Fair Credit Reporting Act (FCRA) and extends the preemption of state law that the FCRA provided. The FTC stated that the FACT Act, "will help reduce identity theft and help victims recover."[33]

HIGHLIGHTS OF SB 473

This legislation is a state effort clearly designed to help reign in identity theft in Texas, to protect Texans from identity thieves, and to give Texans tools to utilize in the event of victimization.

SB 473:

- Prohibits lenders who receive notification of a security alert from extending credit or loaning money without taking reasonable action to verify the consumer's identity.
    - The lender must call the consumer to verify that consumer's identity if the consumer provided the credit reporting agency with a telephone number.
- Allows consumers properly identifying themselves to place a security alert on file with a consumer reporting agency by telephone or in writing.
    - Security alerts are limited to 45 days, but there is no limit to the number of alerts a consumer may place on an account.
- Allows consumers to place a security freeze on their credit file. A security freeze prohibits a consumer reporting agency from releasing a consumer report without the consumer's authorization.
    - Security freezes must be requested in writing by certified mail. A copy of a valid police report, investigative report, or complaint must be included.
    - A security freeze appears to be valid until the consumer removes it.
- As concerns social security numbers, prohibits:
    - Any intentional communication or display.
    - Requiring an individual to transmit their number over an unsecured, unencrypted Internet connection.
    - Any requirement for an individual's number to access an Internet site, unless a password, personal identification number, or other authentication device is also required.
    - Printing an individual's number on any materials, other than a form or application sent by mail, unless the law requires the number in the materials.[34]

HIGHLIGHTS OF THE FACT ACT

The FACT Act places a number of requirements on businesses and grants certain guarantees to consumers. The FTC believes the provisions of the FACT Act, "should help reduce the incidence of identity theft, and help victims recover when the problem does occur."[35]

As relates to identity theft, the FACT Act requires:

- Credit bureaus to provide free annual credit reports to consumers who request them.
- Credit reporting agencies to stop reporting, or to block allegedly fraudulent information resulting from identity theft when the consumer submits an identity theft report.
- Debt collectors who learn that information in a consumer report is the result of identity theft or fraud notify the consumer's creditor or consumer reporting agency.
- Creditors or businesses to provide any consumer who requests them the records of the fraudulent accounts or related transactions associated with the consumer's files.
- Credit and debit card numbers to be truncated.
- The creation of a national fraud alert system that allows consumers who reasonably believe they are the victims of identity theft, or who are military personnel on active duty away from

home, to place an alert on their credit files. The alert warns potential creditors to be cautious when granting credit in that consumer's name.

COMPARING THE LAW

The following table illustrates the major points of each legislative effort as relates to identity theft. The table is certainly not an exhaustive examination of each effort, but instead provides summary information of the key provisions of the bills.

Provision	FACT Act	Texas SB 473
Establishes restriction/restrictions upon when and how a consumer's social security number may or may not be used (the FACT Act contains one very specific restriction; state law contains several to further protect consumers).	√	√
Allows consumer to place some form of alert on their credit file. With an alert on a file, prospective creditors must attempt to contact the person under whose name the credit is applied to verify identity.	√	√
Allows consumers to freeze or block their files with credit reporting agencies under certain conditions. This action places restrictions on what consumer reporting agencies can report. Requires proof of some kind to verify that there is an alleged identity theft.	√	√
Requires truncation of credit card numbers on receipts.	√	
Requires lenders that report negative information to a consumer reporting agency to notify the affected consumers that the lender has, or will report, the negative information.	√	
Under certain circumstances, requires that card issuers verify consumer address changes.	√	
Requires that certain National Credit Union Administration (NCUA), the federal banking agencies, and the FTC to produce procedures to identify potential instances of identity theft.	√	
Requires that furnishers of credit information establish procedures so that information related to identity thefts is not re-reported.	√	
Requires institutions to provide consumers with relevant documents related to an identity theft when such a theft occurs.	√	
Requires credit bureaus to provide free annual credit reports to those who request them.	√	
Establishes federal preemption authority of state law that attempts to enact more strict identity theft laws than contained in the federal statute.	√	

SECTION III: IDENTITY THEFT AND FEDERAL PREEMPTION

Generally, Texas can enact statutes that relate to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, to the extent that those statutes are not inconsistent with any provision of the federal FCRA. Nevertheless, the United States Congress has enacted certain provisions of the federal FCRA that cannot be altered, affected, annulled, or changed by state law. These provisions are set forth under the federal FCRA, 15 U.S.C.A. Section 1681t. There are three recognized forms of federal preemption, each of which is unique: (1) subject matter preemption; (2) disclosure-related preemption; and (3) conduct preemption.

The subject matter preemption prevents states from enacting legally binding laws that address or relate to subjects or topics that are governed by the preemption. As an example, this preemption would annul any state law restricting, limiting, or addressing the information that is available to identity theft victims.

The disclosure-related preemption prevents states from enacting legally binding laws that relate to the certain disclosures controlled by the preemption. As an example, a state cannot enact a statute that addresses the summary of rights of identity theft victims.

The conduct preemption prevents states from enacting legally binding laws that relate to the conduct of certain individuals such as consumer reporting agencies and creditors. Under conduct preemption, state laws that regulated certain conduct by individuals are preempted after the federal law becomes effective. Therefore, a state can enact legally binding statutes until the federal law becomes effective. A perfect example of conduct preemption is the federal preemption pertaining to the truncation of credit card and debit card account numbers. State law pertaining to the truncation of credit card and debit card account numbers will become federally preempted when the federal law becomes effective. The remainder of this section addresses the federally preempted portions of the federal FCRA.

With respect to the federal FCRA, the subject matter preemption relates to:

- prescreening;
- time requirements for a credit reporting agency to take action involving disputes and reinvestigations;
- duties of a person who takes any adverse action with respect to a consumer; information contained in consumer reports (data relevance and obsolescence);
- responsibilities of persons who furnish information to credit reporting agencies;
- affiliate sharing of consumer information, including the use of information for solicitations for marketing purposes;
- information available for identity theft victims; and
- risk-based pricing notice.

With respect to the federal FCRA, the disclosure-related preemption relates to:

- summary of consumer rights to obtain and dispute information in consumer reports;
- summary of rights of identity theft victims;
- information available from businesses to identity theft victims; and
- credit score disclosures by credit bureaus and mortgage lenders.

With respect to the federal FCRA, the conduct preemption relates to:

- truncation of credit card and debit card numbers;

- fraud alerts, extended alert, active duty alerts and their referral among consumer reporting agencies;
- tradeline and other report information blocking by consumer reporting agencies;
- truncation of social security numbers by consumer reporting agencies;
- annual free credit reports by nationwide consumer reporting agencies;
- red flag guidelines for identity theft, prohibiting the sale or transfer of debt caused by identity theft, and debt collector conduct upon notice of identity theft;
- referral by nationwide consumer reporting agencies of file alerts, active duty alerts, blocking and similar actions and annual summary reports to the FTC;
- duties of furnishers upon notice of identity theft-related information; and
- disposal of consumer information.

FEDERAL PREEMPTION SECTION BY SECTION ANALYSIS OF SB 473

The next seven sections will address the federal preemption aspect of the federal FCRA in relation to the provisions enacted as part of SB 473. Section 8 and Section 9 of SB 473 pertain to law enforcement training related to identity theft and are not explored in this analysis. As such, no recommendations are made.

Section 1. Section 20.01, Business & Commerce Code

The first section of SB 473 set forth two new definitions: (1) "security alert" and (2) "security freeze." By itself, these two new definitions for "security alert" and "security freeze" are not federally preempted; however, any actions undertaken to employ the use of these terms are subject to the "conduct preemption." The federal FCRA definition of "fraud alert" is substantially similar to the definition of a "security alert." (15 U.S.C.A. Section 1681c-1). The federal FCRA does not have a provision defining the term of "security freeze" or a similar term. Under Section 20.01 of the Texas Business & Commerce Code, a "security freeze" is defined as "...a notice placed on a consumer file that prohibits a consumer reporting agency from releasing a consumer report relating to the extension of credit involving that consumer file without the express authorization of the consumer." Without defining this term or a similar term, the United States Congress imposed a substantially similar requirement. Under the requirements for extended alerts, if a consumer files an extended fraud alert, a prospective user of a consumer report or of a credit score is prohibited from establishing a new credit plan or extension of credit in the name of the consumer; issuing an additional card on an existing credit account requested by a consumer; or increasing the credit limit on an existing credit account without contacting the consumer by telephone or other reasonable contact method as designated by the consumer. As of December 1, 2004, the FACT Act became effective and the new definitions of extended fraud alerts supersede the need for definitions of security alert and security freeze in SB 473.

Section 2. Section 20.03, Business & Commerce Code

The second section of SB 473 establishes a requirement that a consumer reporting agency must provide, in certain cases, a consumer's right to receive a written disclosure that explains:

- the process for receiving a consumer report or consumer file;
- the process for requesting or removing a security alert or freeze;
- the toll-free telephone number for requesting a security alert;
- applicable fees;
- dispute procedures;
- the process for correcting a consumer file or report; and
- information on a consumer's right to bring an action in court or arbitrate a dispute.

The written disclosures required by this section are subject to the disclosure-related preemption. On November 30, 2004, the FTC promulgated four new or revised written disclosures: (1) the summary of identity theft rights; (2) the general summary of consumer rights; (3) a notice of duties of persons that furnish information to consumer reporting agencies; and (4) a notice of the duties of users of information obtained from consumer reporting agencies. The effective date for these disclosures is January 31, 2005. The first two disclosures, the summary of identity theft rights and the general summary of consumer rights, contain substantially all seven of the elements required by Section 20.03 of the Texas Business & Commerce Code. As of January 31, 2005, the disclosure-related provisions pertaining to Section 20.03 of the Texas Business & Commerce Code are potentially subject to federal preemption.

Section 3. Section 20.031 through 20.039, Business & Commerce Code

The third section of SB 473 addresses the requirements for:

- requesting a security alert;
- a consumer reporting agency to notify a person who requests a consumer report if a security alert is in effect and include a verification telephone number for the person to contact the consumer;
- consumer reporting agencies to maintain a toll-free telephone number for consumers to obtain security alerts;
- requesting a security freeze;
- a consumer reporting agency to notify a consumer, in writing, within 30 calendar days after the change in the consumer's file that the consumer's report has been changed [i.e., the consumer's name, date of birth, social security number, or address];
- a consumer reporting agency to advise a person requesting a consumer report that a security freeze is in place; and
- the removal or temporary lifting of security freeze.

In addition, the third section of SB 473 has two other components: these are exemptions from the security freeze requirements and the requirements for other consumer reporting agencies, other than the notified consumer reporting agency, to honor a security freeze placed on a consumer file by another consumer reporting agency. The provisions found in this section are subject to the conduct preemption. The federal FCRA has identical or similar provisions as Texas law. With the promulgation of the FTC "Identity Theft Rule," all of these provisions are subject to federal preemption. The effective date of this regulation was December 1, 2004.

Section 4. Section 20.04, Business & Commerce Code

The fourth section of SB 473 addresses the permissibility of a consumer reporting agency collecting a fee for placing a security freeze on a consumer file. Additionally, this section was amended to prohibit a consumer reporting agency from charging a fee to a consumer for having a toll-free telephone number dedicated to requesting security alerts. While the federal FCRA does have provisions addressing the cost of purchasing a credit report from the credit reporting agencies, the federal law does not have a provision pertaining to the cost of obtaining a security freeze or an extended fraud alert. In other words, federal law is silent in respect to the permissible fee for a security freeze or an extended fraud alert, if any. The FCRA requires a consumer reporting agency, assuming certain requirements are satisfied, to record an extended fraud alert in the consumer's credit file. The federal law does not appear to permit a consumer reporting agency the authority to refuse an extended fraud alert, assuming the prerequisite elements for the extended fraud alert are satisfied. It appears that a consumer reporting agency would not be allowed to require such a charge before performing the service; however, no definitive ruling has been made on this issue.

Section 5. Section 20.11, 20.12, and 20.13, Business & Commerce Code

The fifth section of SB 473 contains provisions of law that set forth that: (1) injunctive relief that can be sought by the Attorney General of Texas for violations of Chapter 20 of the Texas Business & Commerce Code and the civil penalties for actions brought under this section of law; (2) a violation of Chapter 20 of the Texas Business & Commerce Code is a deceptive trade practices violation under Subchapter E, Chapter 17 of the Texas Business & Commerce Code; and (3) the venue for an action under Chapter 20 of the Texas Business & Commerce Code must be filed in the district court of Travis County; the county in which the violation occurred; or in the county in which the victim resides. The federal FCRA, 15 U.S.C.A. Section 1681s establishes the state action for violations of the federal law and any limitations on state actions for certain violations. In the case of identity theft, the provisions of state law found under Chapter 20 of the Texas Business & Commerce Code are subject to federal preemption, as of December 1, 2004; therefore, any action sought by the Attorney General of Texas or a Texas resident would likely have to be brought under federal law. Consequently, in respect to the identity theft provisions, Section 20.11, 20.12, and 20.13 of the Texas Business & Commerce Code would have no effect; however, they may continue to serve as effective enforcement provisions for the remainder of Chapter 20.

Section 6. Subchapter D, Chapter 35, Texas Business & Commerce Code

The sixth section of SB 473 establishes the requirements for the confidentiality of social security numbers by creating a new section of law, Section 35.58 of the Texas Business & Commerce Code. This section of law indicates a person, other than government or a governmental subdivision or agency, may not:

- intentionally communicate or otherwise make available to the general public an individual's social security number;
- display an individual's social security number on a card or other device required to access a product or service provided by the person;
- require an individual to transmit the individual's social security number over the Internet unless the connection with the Internet is secure or the number is encrypted;
- require an individual's social security number for access to an Internet website, unless a password or unique personal identification number or other authentication device is also required for access; or
- print an individual's social security number on any materials that are sent by mail, unless state or federal law requires that the individual's social security number be included in the materials.

The federal FCRA requires that, at the request of the consumer, consumer reporting agencies must truncate a social security number (first 5 digits of the social security number be excluded) on any disclosure given to the consumer. While the federal FCRA partially governs control of the social security number (truncation of the social security number), the statute does not place any further limitations against other parties. Outside of the federal preemption pertaining to the consumer reporting agencies, it does not appear that the remaining provisions of this section of law are federally preempted by the provisions of the FACT Act.

Section 7. Subchapter D, Chapter 35, Business & Commerce Code

The seventh section of SB 473 involves the verification of the consumer identity in connection with a security alert by enacting a new provision in the law, Section 35.59 of the Texas Business & Commerce Code. This section of law prohibits a person who receives or received a notification of a security alert from lending money, extending credit, or authorizing an application without taking reasonable steps to verify the consumer's identity. Furthermore, the law requires the person receiving the security alert contact the consumer by the specified telephone number given by the consumer when requesting the security alert. Federal law has a nearly identical provision to this state law provision. Under the requirements for extended

alerts, if a consumer files an extended fraud alert, a prospective user of a consumer report or of a credit score is prohibited from establishing a new credit plan or extension of credit in the name of the consumer; issuing an additional card on an existing credit account requested by a consumer; or increasing the credit limit on an existing credit account without contacting the consumer by telephone or other reasonable contact method as designated by the consumer. As of December 1, 2004, the FTC "Identity Theft Rule" became effective; therefore, this section of the bill is now subject to federal preemption.

Other Miscellaneous Issues

In House Bill 235, the Texas Legislature enacted a new statute requiring a person to truncate the credit card and debit card account numbers on electronically printed receipts. Under state law Section 35.58 of the Texas Business & Commerce Code, a person who accepts a credit card or debit card for transactions may not print more than the last four digits of the credit card or debit card account number on a receipt or other document that evidences the transaction and that is provided to the cardholder. In 2003, the United States Congress passed the FACT Act. One section of this law, 15 U.S.C.A. Section 1681c, dealt with the truncation of debit and credit card accounts numbers to five digits for electronically printed receipts. The state law pertaining to the truncation of credit card and debit card account numbers is subject to conduct preemption. For transactions wherein the machine printing the receipts is initially installed and in operation before September 1, 2003, the state statute reflects that the effective date is August 31, 2004. For transactions wherein the machine printing the receipts is installed and in operation after August 31, 2003, the state statute reflects that the effective date is December 31, 2004. Under federal law, the effective dates are December 4, 2004 (if the machine printing the receipt was initially installed and in operation after January 1, 2005) and December 4, 2006 (if the machine printing the receipt was initially installed and in operation before January 1, 2005). Consequently, Texas law would be applicable to electronically printed receipts from August 31, 2004 through December 4, 2004 for machines printing electronic receipts that were installed prior to August 31, 2003 and December 31, 2004 through December 3, 2006 for machines printing electronic receipts that were installed after August 31, 2003. On December 4, 2006, Section 35.58 of the Texas Business & Commerce Code pertaining to the truncation of credit card and debit card account numbers on electronically printed receipts will be completely federally preempted.

SECTION IV: CONCLUSION

In analyzing the identity theft provisions of SB 473, it becomes apparent that many issues addressed by SB 473 are also addressed by the FACT Act. In many cases, the FACT Act identity theft provisions preempt state identity theft law and render those affected provisions of SB 473 substantially less effective, if not completely ineffective.

There are two notable exceptions where consideration of continuation of state law provisions should be observed. The provisions contained in Section 5 of SB 473 pertaining to enforcement actions with respect to other violations of Chapter 20, Business and Commerce Code, is one of those cases. Section 6 governing control of social security numbers as it applies to non-consumer reporting agencies also offers opportunity for continued state regulation.

The rapid growth of identity theft is a continuing and critical issue with which to deal. The Legislature is wise to continue reviewing information related to the crime and taking action when it is required.

1 Identity Theft Resource Center, http://idtheftcenter.org/facts.shtml

2 Federal Trade Commission Testimony before the US House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations. (2003, December 15). Identity Theft: Prevention and Victim Assistance.

3 Ibid.

4 Identity Theft, A publication of the Federal Reserve Bank of Boston, www.bos.frb.org/consumer/identity/index.htm

5 Consumer Reports (2003, October). Stop Thieves from Stealing You.

6 Federal Trade Commission Testimony before the US Senate Special Committee on Aging. (2004, March 23). Efforts to Fight Fraud on the Internet.

7 Ibid.

8 Underwood, Kathyryn (2004, August). As Children Leave Home, Protect Them From Identity Theft. Blethen Maine Newspapers Inc.

9 Federal Trade Commission Testimony before the US Senate Special Committee on Aging. (2004, March 23). Efforts to Fight Fraud on the Internet.

10 Ibid.

11 11 Federal Trade Commission Testimony before the US House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations. (2003, December 15). Identity Theft: Prevention and Victim Assistance.

12 Ibid.

13 Consumer Reports (2003, October). Stop Thieves from Stealing You.

14 Federal Trade Commission. (2004, January 22). National and State Trends in Fraud and Identity Theft. Washington DC, p 7.

15 Ibid, p 3.

16 Ibid.

17 Ibid, p 10.

18 Ibid, p 14.

19 Federal Trade Commission. (2004, January 22). Identity Theft Victim Complaint Data: Figures and Trends in Texas January 1-December 31. 2003. Washington DC.

20 Federal Trade Commission. (2004, January 22). National and State Trends in Fraud and Identity Theft. Washington DC, p 59.

21 Federal Trade Commission. (2004, January 22). Identity Theft Victim Complaint Data: Figures and Trends in Texas January 1-December 31. 2003. Washington DC.

22 Consumer Reports (2003, October). Stop Thieves from Stealing You.

23 Ibid.

24 Ibid.

25 Chipman, Andrea. (2004, April 26). Stealing You. The New York Times, Technology Section, p R8.

26 Ibid.

27 Consumer Reports (2003, October). Stop Thieves from Stealing You.

28 Ibid.

29 Sullivan, Bob. How the Credit Bureaus Helped the Biggest Identity Theft in History. MSNBC.com, 2003, http://www.msnbc.msn.com/id/5800052/

30 Sullivan, Bob. ID Thief to the Stars Tells All. MSNBC.com, 2003, http://www.msnbc.msn.com/id/5763781/

31 Sullivan, Bob. He was Paul Allen for a While. MSNBC.com, 2003, http://www.msnbc.msn.com/id/5800044/

32 Identity Theft, A publication of the Federal Reserve Bank of Boston, www.bos.frb.org/consumer/identity/index.htm

33 Press Release issued by the Federal Trade Commission, June 15, 2004.

34 Ibid.

35 Ibid.