The Bill Blackwood
Law Enforcement Management Institute of Texas

==========

Police Response to the Identity Theft Crisis

==========

An Administrative Research Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

==========

By
Craig Fos

Dickinson Police Department
Dickinson, Texas
October 2006

ABSTRACT

Identity theft is one of the fastest growing problems facing this nation. The recovery process for a victim of identity theft can be an extremely long process. The recovery process begins with filing a police report, which, at times, can be a grueling process. Questions regarding jurisdiction often cause police officers to refer victims to other agencies. The purpose of this research paper was to determine how police officers are responding to local identity theft victims when they attempt to report the crime when the financial loss occurs in another jurisdiction. It was found that about six percent of the officers do not take a report from the victim. Twenty-nine to forty percent of the officers do take a report from the victim. However the victim is often told to make an additional report with the agency where the financial loss occurred. This demonstrates a need for change in the way many officers are handling identity theft victims.

TABLE OF CONTENTS

Page

INTRODUCTION

Identity theft is one of the fastest growing problems facing this nation. The aforementioned crime is committed when a person fraudulently uses another's individual's identification information to obtain credit, merchandise, or services in the name of the victim. The Federal Trade Commission's Consumer Sentinel received 246,570 reports of identity theft in 2004. This was an almost 700% increase from the 31,103 reported cases in 2000. (Federal Trade Commission, 2005). Prior to 1999, in Texas, a victim of identity theft had little standing. The law classified the victim to be the person who suffered the financial loss. Any restitution ordered in an identity theft case was made to the financial loss victim as well.

This shortcoming was addressed by the Texas state legislature in 1999. In the 76th session of the Texas State Legislature a bill was passed adding Section 32.51 to the Texas Penal Code. This law was titled "Fraudulent Use or Possession of Identifying Information." This statute makes it unlawful to use another person's identifying information without his/her consent when done with the intent to harm or defraud another. It also allows the victim to receive compensation for lost wages and other expenses incurred as a result of the crime.

As of 1999, victims of identity theft now have standing, however the venue of the crime was still held in the county where the economic loss was incurred. This meant that the victim of identity theft had to contact the agency where the economic loss occurred to make an offense report. This has proven to be problematic because numerous agencies refuse to take offense reports by phone. If a victim is located across the state from where the financial loss occurred, this could become an

insurmountable problem. In 2003, the 78th session of the Texas State Legislature amended the Code of Criminal Procedure to allow for prosecution in the county in which the crime occurred, or the county in which the victim resides.

While, in theory, a victim of identify theft should be able to report the crime to the police agency in whose jurisdiction they reside, this may not be the case. Nationally, in 2004, 93,578 victims attempted to report an identity theft case to the police. Twenty percent of theses victims, or 19,195, were not able to make report. (Federal Trade Commission, 2005).

The purpose of this research paper will be to determine whether police officers in Texas are taking reports from local identity theft victims if the financial lose occurred in a different jurisdiction. This research will also attempt to determine, from officers that do take identity theft reports, will they also refer the victims to the agency with jurisdiction where the financial loss occurred to make additional reports thus adding to the time needed for the victim to recover from the crime. Research will be conducted by reviewing publications, legislation and statutes with regards to identity theft. Additionally, officers of various ranks from departments throughout Texas will be surveyed regarding their response to reports of identity theft. It is believed a significant number will admit to referring victims to the jurisdiction(s) where the financial loss occurred, thus causing the victim additional work in an already trying time.

It is the hope of this author the results of this research will impress upon police administrators that most police departments have a lack of understanding regarding jurisdiction in identity theft cases. However, with the information presented here,

administrators within their respective departments will be able to use this information develop or clarify proper procedures for dealing with victims of identity theft.

REVIEW OF LITERATURE

The victim of a residential burglary generally discovers the crime shortly after it occurs. Typically, the victim would come home, find signs that forced entry to their residence had occurred, and find some of their valuables missing. For these unfortunate souls, in order to make a police report, they would simply call the police or sheriff's department that has jurisdiction in the location of their residence.

In contrast to a burglary victim the victim of an identity theft, may not discover the crime for months or even years after the crime has occurred. Often the first indication a crime has occurred is a letter from a collection agency trying to collect a debt the victim never incurred. Collection agencies will track the victim down at their real address, and not the address used by the criminal when the victim's identity was used to open the credit account.

Victims often met with resistance from the police when they attempted to file a police report. In fact, in Texas, they did not have standing as the victim of the crime until 1999. Starting that year the victim had standing, but the venue for the crime was still held in the county where the financial loss occurred. In 2003 the law was changed to allow venue in the county where the victim resides. Despite this, many officers would refer the victim to the location where the financial loss occurred. All of the literature for identity theft victims stresses the importance of making a police report.

In an article on identity theft found the August 2001 issue of Ebony magazine it was stated that:

> First and foremost, call the police. In cases of identity theft and illegal credit card use, it's especially important to get a police report. However, some officers won't write a report. They claim that the credit card company--not the consumer--is the true victim of the fraud because it absorbs the financial losses. Be persistent, says Gregg McClain, chief of the economic fraud and environmental protection unit in the district attorney's office of San Diego. Don't leave the station without something in writing. (n.p.)

In March of 2005, Arthur Hendricks of North Richland Hills, Texas, received a notification from the IRS that he owed $37,242 in back taxes, penalties and interest. The letter indicated that he owed the taxes on unreported income from a job that he had worked in Virginia in 2003. Hendricks had not worked in Virginia. Hendricks went to his local police department and tried to make a police report. They were sympathetic, even giving him a brochure on identity theft, but they would not take a report. Calls to the Virginia State Police and the police in the county where the suspect was working received similar results. Hendricks contacted the local FBI office and was told that they would assist in the case, but only if requested by the local police. He was finally able get the IRS Problem Resolution Hotline to clear the debt off of his IRS account. He still wants criminal charges filed on the suspect, but without a police agency to investigate, this will not happen. (Fort Worth Star-Telegraph April, 2005).

This author interviewed victim, who will be referred to as “Kim”. In December of 2004 Kim received a collection notice on a credit account that she had not opened. A credit report revealed several other accounts that were opened without her knowledge. The police were called and a multi-agency investigation was begun. Eventually four separate police departments in two different counties became involved in the investigation. Kim’s identifying information had been used to purchase a big screen TV, clothing, electronic equipment, toys, residential phone service, cell phone service, and electrical service. One of the suspects even used her identity to secure a loan to pay for breast augmentation surgery.

It was discovered that over fifteen credit accounts had been opened using the Kim’s name, amassing a debt in excess of $29,000.00. Kim had to contact each of these creditors to clear the debt from her name. In each instance there was a matrix of computer-generated options prior to speaking to a live person. Normally she was transferred to a second department before she could make a report. Follow-up written documentation was required. Over time this became a very frustrating and time-consuming endeavor. A couple of months after the investigation was completed one of the creditors sent a letter to Kim stating that their investigation revealed that no fraud had taken place and offering to set the victim up on a payment plan to resolve the debt. This was so unsettling that Kim considered filing for bankruptcy. Kim contacted the investigator who had worked on her case and he was able to make contact with the creditor. He explained that a fraud had indeed taken place and that criminal charges had been filed against six suspects. The debt was eventually cleared from her name.

Kim had not originally contacted the police department that had jurisdiction over the area where she lived. Had she contacted them first she would have been saved from contacting so many police departments. After she had made a report with her hometown police agency, another account was discovered that had been opened in a fifth city. Charges stemming from that offense were filed by her hometown police agency.

In another case, State Sen. Juan “Chuy” Hinojosa, D-McAllen, had a staff members, Mary Lou Conner, who was the victim of an identity theft. She spent hours and hours during the day on the phone trying to clear her name and it eventually took over three years to get the matter resolved. As a result of this Hinojosa introduced legislation, (Senate Bill 122), giving the Attorney General’s Office authority to take civil action against those who engage in identity theft and the ability to take action against businesses that do not safeguard personal identifying information. This law also requires that police officer are to take reports from victims of identity theft. The victim can request a copy of the report, which must include the results of the investigation. (Attorney General Abbott, 2005). This legislation passed and now affect all identity thefts that occur after September 1, 2005.

METHODOLGY

The purpose of this research paper will be to determine whether police officers are taking reports from local identity theft victims if the financial loss occurred in a different jurisdiction. It will also try to determine if the victims are being instructed to contact additional police agencies, adding to the time needed to recover from the crime.

It is the author's belief that some officers will refuse to take any report and even more will refer the victims to make an additional report with a second agency.

FINDINGS

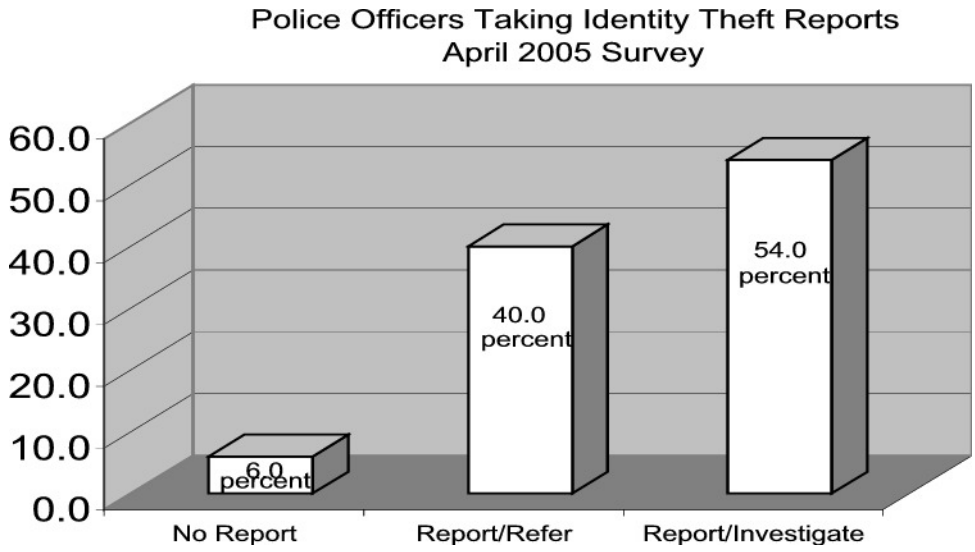
In April of 2005, a survey was conducted between two groups. The first group consisted of the author's fellow students at the Law Enforcement Management Institute (LEMIT), Module I class. The second group was made up of officers working an entertainment event. This group consisted of officer from agencies spread out over southeast Texas. Since the aforementioned survey was longer, they were hand delivered to the officers and the author waited for them to complete them. This resulted in a 100% return rate.

Since the passage of Senate Bill 122 changed the legal requirements regarding identity theft reporting, a second survey was taken one year later in April of 2006. This survey was submitted to officers again working an entertainment event. The group consisted of officers from agencies spread out over southeast Texas. Again the surveys were hand delivered to the officers and the author waited for them to complete them. Two of the surveys were not returned because those officers received several calls for service before they could complete and turn in the survey form. This resulted in a 96% return rate on the April 2006 survey.

During the initial survey in April of 2005 fifty officers representing twenty-eight different police agencies were surveyed. The departments ranged in size from four officers (Haskell Police Department) to 5300 officers (Houston Police Department). Ranks included police officer/deputy, detective, sergeant, lieutenant, captain, and chief. The majority of the officers, thirty, were assigned to the patrol division of their

department. The remainders of the officers were assigned to criminal investigation, administration, training, recruiting, or the jail.

The officers involved in these surveys were all aware of the rise in identity theft reports. It was surprising to this author, that only 6% of the respondents would not take any police report from an identity theft victim where the financial loss occurred in a different county. Forty percent would at least take a report, but would advise the victim to make additional reports with the agency having jurisdiction where the financial loss took place. The majority, 54% would take a report and advise the victim that their department would handle any follow-up investigation.



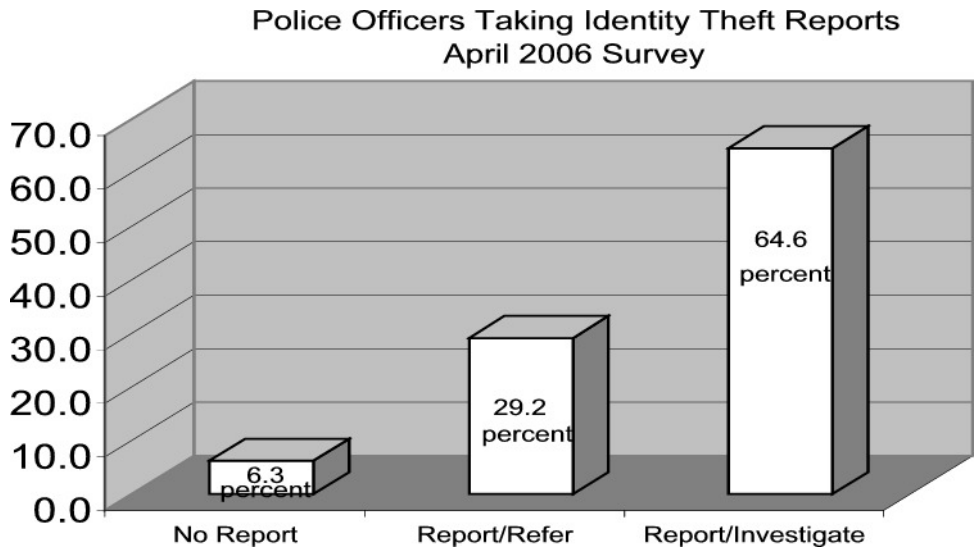
There was no significant difference in the responses if the financial loss occurred in another state. Only two officers gave different answers, one taking a report and referring the victim when the financial loss was out of county and the other taking a report and investigating it when the financial loss was out of state. The second officer gave the opposite answers.

Several of the investigators who indicated that their agency would investigate the crimes noted that they would need assistance from the agencies where the financial loss occurred. Some even indicating that they would refer the investigation to the other agency, but noting that they would not expect the victim to have to make contact with the agency. Senate Bill 122 changed the law regarding the reporting of identity theft crimes. Specifically the law requires that an officer take a report when contacted by a victim. Since this law took effect after the first survey this author decided to conduct a second survey to see if Senate Bill 122 had an significant influence on the answers.

The second survey was conducted in April of 2006. Fifty officers representing eighteen agencies were surveyed. Two did not complete the survey. The departments ranged in size from five officers (Huntington and Surfside Police Departments) to 5300 officers (Houston Police Department). Ranks included police officer/deputy, corporal, detective, sergeant, lieutenant, captain, deputy chief, and chief. The majority of the officers, thirty-two, were assigned to the patrol division of their department. The remainder were assigned to criminal investigation, civil, training, or transport.

The second survey showed no significant change in the number of officers who would not take any report at all when the financial loss occurred in another county, with 6.3% responding this way. There was a significant decrease in the number of officers who would take a report and then refer the victim to the agency where the financial loss occurred. The survey results indicated that only twenty-nine percent would refer the victim to make an additional report. This was down by eleven percent over the April 2005 survey. The number of respondents who would take the report and advise the

victim that their department would conduct the investigation increased from fifty-four percent to almost sixty-five percent.



The fact that the financial loss occurred out of state did make more of a difference in the 2006 survey as opposed to the 2005 survey. The number of officers who would not take an identity theft report dropped to 4.2%. The number of officers who would take a report and also advise the victim to make an additional report rose to 35.4%. The number of officers who would take the report and advise the victim that their department would conduct the follow-up investigation dropped back to 60.4%. This was still an increase of over six percent from the 2005 survey.

It should be noted that the officers who indicated that they would not take any report were advised of the change in the law requiring them to take a report. Most officers surveyed in April 2006 stated that they were not aware of the change in the law.

DISCUSSION

Identity theft is a crime that can take a long time to recover from. The victims can spend hours on the phone trying to get charges that they did not make removed from their name. Many creditors require a police report before they will remove the debt. At times victims have had a difficult time getting the police to take a report. This research paper was conducted to determine whether police officers are taking reports from local identity theft victims if the financial loss occurred in a different jurisdiction. This paper also attempted to determine if, when a report is taken, are the victims also being instructed by the officer to contact additional police agencies, as these additional contacts add to the time needed to recover from the crime. It Is this author's belief at the outset of this research paper that some officers would refuse to take any report. In addition, it was premised that even more would refer the victim to make an additional report with a second agency. The results of this research survey indicated that the vast majority of police officers that were contacted would take a report from the victim of identity theft. However, way too many, twenty-nine to forty percent, will still refer the victim to make an additional report. The decrease that was noted between the two surveys numbers in one year is a move in the right direction.

Police administrators should be ever conscience of the demands made on identity theft victims. Departments, through policy and procedures, should attempt to reduce the time that it takes for the victims' to get their lives back to normal. It's critical that Departments develop and implement policies requiring officer to assist identity theft victims with their recovery. No officer in this state should be allowed to refuse to take a

report from an identity theft victim. In addition, victims should not be forced to make additional reports to multiple police agencies.

Senate Bill 122 goes a long way towards combating identity theft, however because of internet purchasing, on-line banking and unsecured access to personal information, this crime will continue to rise in the future. Non-personal purchases are on the rise. There are gasoline purchases being made at the pumps using credit cards, groceries are paid for at self-serve registers without a cashier's interaction and more and more purchases are being made over the Internet. When there is no personal interaction it is easier to use someone else's credit to purchase goods.

What may be required is a statewide task force. As with narcotic type crimes, these illegal activities consistently cross many police jurisdictions. Thus in the 1980's multi-agency task forces were formed to combat this problem. In the 1990's auto crime task forces were formed to combat the organized auto theft trade. Therefore, the time may have come for the formation of multi-agency identity theft task forces. A statewide network could be more effective in the investigation of this crime that knows no borders.

REFERENCES

Attorney general abbott applauds new measure to fight identity theft in texas. (2005, February). Texas Attorney General's Office. Retrieved April 13, 2005, from: http://www.oag.state.tx.us/oagnews/release.php?id=791

Dadisho, E. (2005, January). Identity theft and the police response: the problem. *Police Chief* , 72 (1) 25-29, 72 (2) 17-26, 72 (3) 46-52.

Eaton, T. (2005, March 23). Hinojosa proposes legislation to help curb identity theft. *Corpus Christi Caller-Times*, B4.

Federal Trade Commission. (2005). National and state trends in fraud & identity theft, January - December 2004. Retrieved April 9, 2005, from http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf

Federal Trade Commission. (2001). *Figures and trends on identity theft*. January 2000 through December 2000. Retrieved April 9, 2005, from http://www.ftc.gov/bcp/workshops/idtheft/charts-update.pdf

Identity theft: how to fight the scam - brief article. (2001, August). *Ebony.*

Identity theft victims skyrocket. (2003, November). *Information Management Journal.*

Lieber, D. (2005, April 1). Identity theft tough to straighten out. *Fort Worth Star-Telegram*, 1B.

Schmalleger, F. (2005). Criminal Justice Today (8th Ed.).Upper Saddle River: Pearson Prentice Hall.

Texas Penal Code. (2003). Section § 32.51. Fraudulent use or possession of identifying information. Retrieved April 13, 2005,from: www.Capitol.state.tx.us/statutes/docs/PE/content/htm/pe.007.00.000032.00.htm

Texas Code of Criminal Procedure. (2003). Article 13.28-Fraudulent use or possession of identifying information. Retrieved April 13, 2005, from: www.capitol.state.tx.us/statutes/docs/CR/content/htm/cr.001.00.000013.00.htm

APPENDIX

PENAL CODE: CHAPTER 32--FRAUD

§ 32.51. FRAUDULENT USE OR POSSESSION OF IDENTIFYING INFORMATION. (a) In this section:

(1) "Identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

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

(B) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(C) unique electronic identification number, address, and routing code, financial institution account number; and

(D) telecommunication identifying information or access device.

(2) "Telecommunication access device" means a card, plate, code, account number, personal identification number, electronic serial number, mobile identification number, or other telecommunications service, equipment, or instrument identifier or means of account access that alone or in conjunction with another telecommunication access device may be used to:

(A) obtain money, goods, services, or other thing of value; or

(B) initiate a transfer of funds other than a transfer originated solely by paper instrument.

(b) A person commits an offense if the person obtains, possesses, transfers, or uses identifying information of another person without the other person's consent and with intent to harm or defraud another.

(c) An offense under this section is a state jail felony.

(d) If a court orders a defendant convicted of an offense under this section to make restitution to the victim of the offense, 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.

(e) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section or the other law.

Added by Acts 1999, 76th Leg., ch. 1159, § 1, eff. Sept. 1, 1999. Amended by Acts 2003, 78th Leg., ch. 1104, § 4, eff. Sept. 1, 2003.

CODE OF CRIMINAL PROCEDURE

CHAPTER 13--VENUE

Art. 13.28. Fraudulent Use or Possession of Identifying Information

Text of article as added by Acts 2003, 78th Leg., ch. 415, Sec. 1

An offense under Section 32.51, Penal Code, may be prosecuted in any county in which the offense was committed or in the county of residence for the person whose identifying information was fraudulently obtained, possessed, transferred, or used.

Added by Acts 2003, 78th Leg., ch. 415, Sec. 1, eff. Sept. 1, 2003.

For text of article as added by Acts 2003, 78th Leg., ch. 392, Sec. 1, see art. 13.28, ante.

CODE OF CRIMINAL PROCEDURE

CHAPTER 2--GENERAL DUTIES OF OFFICERS

Art. 2.29. REPORT REQUIRED IN CONNECTION WITH FRAUDULENT USE OR POSSESSION OF IDENTIFYING INFORMATION. (a) A peace officer to whom an alleged violation of Section 32.51, Penal Code, is reported shall make a written report to the law enforcement agency that employs the peace officer that includes the following information:

(1) the name of the victim;

(2) the name of the suspect, if known;

(3) the type of identifying information obtained, possessed, transferred, or used in violation of Section 32.51, Penal Code; and

(4) the results of any investigation.

(b) On the victim's request, the law enforcement agency shall provide the report created under Subsection (a) to the victim. In providing the report, the law enforcement agency shall

redact any otherwise confidential information that is included in the report, other than the information described by Subsection (a).

Added by Acts 2005, 79th Leg., ch. 294, Sec. 1(a), eff. Sept. 1, 2005.

S.B. No. 122

AN ACT

relating to the prevention and punishment of identity theft and the rights of certain victims of identity theft; providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. (a) Chapter 2, Code of Criminal Procedure, is amended by adding Article 2.29 to read as follows:

Art. 2.29. REPORT REQUIRED IN CONNECTION WITH FRAUDULENT USE OR POSSESSION OF IDENTIFYING INFORMATION. (a) A peace officer to whom an alleged violation of Section 32.51, Penal Code, is reported shall make a written report to the law enforcement agency that employs the peace officer that includes the following information:

(1) the name of the victim;

(2) the name of the suspect, if known;

(3) the type of identifying information obtained, possessed, transferred, or used in violation of Section 32.51, Penal Code; and

(4) the results of any investigation.

(b) On the victim's request, the law enforcement agency shall provide the report created under Subsection (a) to the victim. In providing the report, the law enforcement agency shall redact any otherwise confidential information that is included in the report, other than the information described by Subsection (a).

(b) The change in law made by this section applies only to the investigation of an offense committed on or after September 1, 2005. The investigation of an offense committed before September 1, 2005, is covered by the law in effect when the offense was committed, and the former law is continued in effect for that purpose. For purposes of this subsection, an offense is committed before September 1, 2005, if any element of the offense occurs before that date.

SECTION 2. Title 4, Business & Commerce Code, is amended by adding Chapter 48 to read as follows:

CHAPTER 48. UNAUTHORIZED USE OF IDENTIFYING INFORMATION

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 48.001. SHORT TITLE. This chapter may be cited as the Identity Theft Enforcement and Protection Act.

Sec. 48.002. DEFINITIONS. In this chapter:

(1) "Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;

(B) mother's maiden name;

(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(D) unique electronic identification number, address, or routing code; and

(E) telecommunication access device.

(2) "Sensitive personal information":

(A) means an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and

(B) does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

(3) "Telecommunication access device" has the meaning assigned by Section 32.51, Penal Code.

(4) "Victim" means a person whose identifying information is used by an unauthorized person.

[Sections 48.003-48.100 reserved for expansion]

SUBCHAPTER B. IDENTITY THEFT

Sec. 48.101. UNAUTHORIZED USE OR POSSESSION OF PERSONAL IDENTIFYING INFORMATION. (a) A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good,

a service, insurance, an extension of credit, or any other thing of value in the other person's name.

(b) It is a defense to an action brought under this section that an act by a person:

(1) is covered by the Fair Credit Reporting Act (15 U.S.C. Section 1681 et seq.); and

(2) is in compliance with that Act and regulations adopted under that Act.

(c) This section does not apply to:

(1) a financial institution as defined by 15 U.S.C. Section 6809; or

(2) a covered entity as defined by Section 601.001 or 602.001, Insurance Code.

Sec. 48.102. BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION. (a) A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.

(b) A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:

(1) shredding;

(2) erasing; or

(3) otherwise modifying the sensitive personal information in the records to make the information unreadable or undecipherable through any means.

(c) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

Sec. 48.103. NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA. (a) In this section, "breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person. Good faith acquisition of sensitive personal information by an employee or agent of the person or business for the purposes of the person is not a breach of system security unless the sensitive personal information is used or disclosed by the person in an unauthorized manner.

(b) A person that conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any resident of this state whose sensitive personal information was, or

is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(c) Any person that maintains computerized data that includes sensitive personal information that the person does not own shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(d) A person may delay providing notice as required by Subsections (b) and (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that it will not compromise the investigation.

(e) A person may give notice as required by Subsections (b) and (c) by providing:

(1) written notice;

(2) electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or

(3) notice as provided by Subsection (f).

(f) If the person or business demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information, the notice may be given by:

(1) electronic mail, if the person has an electronic mail address for the affected persons;

(2) conspicuous posting of the notice on the person's website; or

(3) notice published in or broadcast on major statewide media.

(g) Notwithstanding Subsection (e), a person that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person notifies affected persons in accordance with that policy.

(h) If a person is required by this section to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. Section 1681a, that maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

[Sections 48.104-48.200 reserved for expansion]

SUBCHAPTER C. REMEDIES AND OFFENSES

Sec. 48.201. CIVIL PENALTY; INJUNCTION. (a) A person who violates this chapter is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring suit to recover the civil penalty imposed by this subsection.

(b) If it appears to the attorney general that a person is engaging in, has engaged in, or is about to engage in conduct that violates this chapter, the attorney general may bring an action in the name of this state against the person to restrain the violation by a temporary restraining order or a permanent or temporary injunction.

(c) An action brought under Subsection (b) shall be filed in a district court in Travis County or:

(1) in any county in which the violation occurred; or

(2) in the county in which the victim resides, regardless of whether the alleged violator has resided, worked, or done business in the county in which the victim resides.

(d) The plaintiff in an action under this section is not required to give a bond. The court may also grant any other equitable relief that the court considers appropriate to prevent any additional harm to a victim of identity theft or a further violation of this chapter or to satisfy any judgment entered against the defendant, including the issuance of an order to appoint a receiver, sequester assets, correct a public or private record, or prevent the dissipation of a victim's assets.

(e) The attorney general is entitled to recover reasonable expenses incurred in obtaining injunctive relief, civil penalties, or both, under this section, including reasonable attorney's fees, court costs, and investigatory costs. Amounts collected by the attorney general under this section shall be deposited in the general revenue fund and may be appropriated only for the investigation and prosecution of other cases under this chapter.

(f) The fees associated with an action under this section are the same as in a civil case, but the fees may be assessed only against the defendant.

Sec. 48.202. COURT ORDER TO DECLARE INDIVIDUAL A VICTIM OF IDENTITY THEFT. (a) A person who is injured by a violation of Section 48.101 or who has filed a criminal complaint alleging commission of an offense under Section 32.51, Penal Code, may file an application with a district court for the issuance of a court order declaring that the person is a victim of identity theft. A

person may file an application under this section regardless of whether the person is able to identify each person who allegedly transferred or used the person's identifying information in an unlawful manner.

(b) A person is presumed to be a victim of identity theft under this section if the person charged with an offense under Section 32.51, Penal Code, is convicted of the offense.

(c) After notice and hearing, if the court is satisfied by a preponderance of the evidence that the applicant has been injured by a violation of Section 48.101 or is the victim of an offense under Section 32.51, Penal Code, the court shall enter an order containing:

(1) a declaration that the person filing the application is a victim of identity theft resulting from a violation of Section 48.101 or an offense under Section 32.51, Penal Code, as appropriate;

(2) any known information identifying the violator or person charged with the offense;

(3) the specific personal identifying information and any related document used to commit the alleged violation or offense; and

(4) information identifying any financial account or transaction affected by the alleged violation or offense, including:

(A) the name of the financial institution in which the account is established or of the merchant involved in the transaction, as appropriate;

(B) any relevant account numbers;

(C) the dollar amount of the account or transaction affected by the alleged violation or offense; and

(D) the date of the alleged violation or offense.

(d) An order rendered under this section must be sealed because of the confidential nature of the information required to be included in the order. The order may be opened and the order or a copy of the order may be released only:

(1) to the proper officials in a civil proceeding brought by or against the victim arising or resulting from a violation of this chapter, including a proceeding to set aside a judgment obtained against the victim;

(2) to the victim for the purpose of submitting the copy of the order to a governmental entity or private business to:

(A) prove that a financial transaction or account of the victim was directly affected by a violation of this chapter or the commission of an offense under Section 32.51, Penal Code; or

(B) correct any record of the entity or business that contains inaccurate or false information as a result of the

violation or offense;

(3) on order of the judge; or

(4) as otherwise required or provided by law.

(e) A court at any time may vacate an order issued under this section if the court finds that the application or any information submitted to the court by the applicant contains a fraudulent misrepresentation or a material misrepresentation of fact.

(f) A copy of an order provided to a person under Subsection (d)(1) must remain sealed throughout and after the civil proceeding. Information contained in a copy of an order provided to a governmental entity or business under Subsection (d)(2) is confidential and may not be released to another person except as otherwise required or provided by law.

Sec. 48.203. DECEPTIVE TRADE PRACTICE. A violation of Section 48.101 is a deceptive trade practice actionable under Subchapter E, Chapter 17.

SECTION 3. This Act takes effect September 1, 2005.

_____ _____

President of the Senate Speaker of the House

I hereby certify that S.B. No. 122 passed the Senate on April 21, 2005, by the following vote: Yeas 31, Nays 0; May 17, 2005, Senate refused to concur in House amendments and requested appointment of Conference Committee; May 20, 2005, House granted request of the Senate; May 26, 2005, Senate adopted Conference Committee Report by the following vote: Yeas 31, Nays 0.

_____

Secretary of the Senate

I hereby certify that S.B. No. 122 passed the House, with amendments, on May 13, 2005, by a non-record vote; May 20, 2005, House granted request of the Senate for appointment of Conference Committee; May 27, 2005, House adopted Conference Committee Report by the following vote: Yeas 142, Nays 0, two present not voting.

_____

Chief Clerk of the House

Approved:

_____
Date

_____

SURVEY

A survey was prepared containing brief biographical information and the following two questions:

A local resident comes to your department reporting that their identity has been stolen and used to open credit cards. These credit cards were used to make purchases at stores in a neighboring county. Would you, or an officer with your department:

- ☐ A) Offer your condolences and refer them to the agencies in the locations where the card was used.
- ☐ B) Take a report for informational purposes and then refer them to make an additional report for investigative purposes in the location where the card was used.
- ☐ C) Take a report and advise them that your department would conduct the follow-up investigation on the case.

A local resident comes to your department reporting that their identity has been stolen and used to open credit cards. These credit cards were used to make purchases at stores in a different state. Would you, or an officer with your department:

- ☐ A) Offer your condolences and refer them to the agencies in the locations where the card was used.
- ☐ B) Take a report for informational purposes and then refer them to make an additional report for investigative purposes in the location where the card was used.
- ☐ C) Take a report and advise them that your department would conduct the follow-up investigation on the case.