The Bill Blackwood
Law Enforcement Management Institute of Texas

=====

A Stolen Life:
Identity Theft and How It Affects You

=====

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

=====

By
Brian C. Williams

Texas Alcoholic Beverage Commission
Lubbock, Texas
July 2008

ABSTRACT

Identity theft is a fast growing crime that can occur in many different ways. It is not only difficult for a person to protect themselves from becoming victims, but it is also hard for law enforcement officers to investigate identity theft due to a lack of training. To prove this point, various journals, articles, publications, and internet sites will be reviewed to find the information necessary to prove these claims. After researching this subject, it was discovered that identity theft is the fastest growing crime facing law enforcement and the average citizen, today. A need for more specialized training for officers was found to be not only necessary, but desired by many officers in order to help them investigate these crimes more efficiently.   After all of the data was compiled and reviewed, the author's original concept validated that identity theft is a problem and that advanced training and education regarding the subject can foster the prevention of such a crime.

TABLE OF CONTENTS

Page

Abstract

INTRODUCTION

What is identity theft? Twenty years ago, this phrase was not heard often in either the civilian or law enforcement community. Usually, when someone said they had had their identity stolen, most people assumed the person meant someone had used their name and pretended to be them. Today, the term identity theft means so much more. Not only are people's names being stolen, but almost any item of personal information about them. Perhaps more disturbing is the fact that until recently, law enforcement has largely ignored this problem due to either not understanding what identity theft really is or because of a lack of training and the resources necessary to pursue the criminal case.

With the creation of the World Wide Web, and the subsequent use of home computers, identity theft has flourished in the last ten years. With the simple click of a button, an individual can find out everything from a person's name, social security number, date of birth, driver's license number or just about any other bit of information that most people think of as being private. Worse yet, the same individual who obtains this information can then use it to open up charge accounts, apply for and receive credit cards or even buy homes in someone else's name. More disturbing than this is the ease in which they can obtain these things from companies who have no idea that theft if being committed. Billions of dollars are being lost each year to identity theft in the retail and business world.

Only within the last few years has law enforcement recognized the threat that identity theft poses not only to individuals, but to Homeland security as well. Ask most officers today what identity theft is, and it is likely to generate a different answer from

each one. Furthermore, if it were asked of the same officers how many had received training in this area many would respond that they had little to no training in dealing with identity theft. The good news is that more and more law enforcement agencies are recognizing the growing problem of identity theft and are attempting to train their officers to better investigate these incidents as they occur.

The author's intent in conducting this research is twofold; the first being to identify the various forms of identity theft and the second is to establish the need for better training by law enforcement agencies regarding this issue. Is the officer on the street really aware of the various ways that identity theft occurs and, more importantly, do they know what to tell the victims of identity theft?   The author intends to use several methods of inquiry to accomplish these goals. Research of various journals, books, reports and inquiries on the internet will be used to obtain the information needed. In addition, the author anticipates conducting a survey of police officers in reference to their knowledge and training about identity theft.

By identifying the various forms of identity theft and what training is currently being done in this area, the author believes that the results of this research will benefit both the law enforcement community as well as the individual officer who will ultimately investigate the offense. More importantly, the author intends to give anyone who reads this paper, an idea of what identity theft is and some tips on how to protect themselves from it happening to them.

REVIEW OF LITERATURE

According to a survey conducted in January of 2005 by the United States Department of Justice, 9.3 million Americans were the victims of identity theft in 2004.

The survey also concluded that most of the information stolen by the thieves was stolen by traditional, rather than electronic means. The Federal Trade Commission gives some insight into how thieves obtain personal information. Often, thieves may steal mail such as bank statements and bills, giving them access to vital information such as bank accounts, credit accounts and utilities—all of which contain the information necessary to commit identity theft. They may also complete a change of address form at the post office and then use the information obtained to open new, or charge to, existing accounts. "Dumpster Diving" is also a popular way to find and then sort through your garbage for information. Of course, there are still the traditional ways to obtain someone else's information such as stealing a wallet or purse, eavesdropping on conversations, stealing information directly from a residence or by "phishing" which is using the telephone or internet to pose as legitimate companies needing information vital to individual credit accounts ("Take Charge", 2005).

Of all of the instances of identity theft reported in 2004, seventy percent started with the theft of personal data by employees where they were employed (Pavlicek, 2005). For those businesses that utilize credit reports, it is all too easy for employees wishing to commit identity theft to obtain almost any individual's credit report. At retail stores, accounts may be "skimmed" which is when the data on the back of a credit or debit card is stored to a data device when the card is swiped for an actual purchase ("Take Charge", 2005). Once information has been stolen, it can be used to do almost anything imaginable. It is not uncommon for identity thieves to open up charge accounts, bank accounts or even have utilities turned on in someone else's name.

There have even been cases where thieves have bought cars and houses using someone else's name and credit.

Even though money is the number one reason behind stealing someone else's identity, it is not the only one. Since 9/11, there has been an increase in the number of identity thefts that have resulted in people using another person's name, date of birth and social security number to obtain fraudulent driver's licenses, duplicate social security numbers and even apply for, and receive, jobs. There have even been instances of fraudulent tax returns and even bankruptcy cases filed using stolen identities ("Take Charge", 2005).

The National Crime Prevention Council reported that, on average, it takes a consumer who has been the victim of identity theft 30 hours and $500 to clean up their credit reports and name with the average financial loss being $1440 (National Crime Prevention Council, 2005). In this same study, credit card fraud was reported to be the most common form of identity theft. This was followed by utility fraud and then bank fraud. On a per capita ratio, Arizona, California and Nevada lead the nation as having the highest incidents of identity theft, with Colorado, Texas, Florida, New York, Washington, Illinois and Oregon rounding out the top 10. Furthermore, 18 to 29 year olds are the most targeted population group as victims of identity theft, but there is a growing trend at targeting the elderly.

Based on this information, it is easy to see that identity theft has been on a steady increase in the last several years. Law enforcement has also noticed this disturbing trend and has taken steps to address the issue. However, many officers believe that few cases of identity theft are actually solved. This is due to the anonymity

of the crime, jurisdiction issues, lax security measures on behalf of all involved and the lack of cooperation by the credit industry and law enforcement agencies (Dadisho, 2005). Dadisho also cited a 2003 study by the Calprig Education Fund, which also found that most identity theft crimes are never solved, for almost the same reasons stated in the 2005 study Dadisho conducted. The Calprig study also concluded that new policies are needed to assist law enforcement agencies in working and prosecuting identity theft crimes. Also, more cooperation between law enforcement and financial institutions was noted as being key in working toward identifying identity thieves.

In 2004, the Journal of Economic Crime Management recommended 7 items that were aimed to create a comprehensive national and global strategy to combat identity theft. They were: in a commitment from the highest levels of federal government to lead and fund a national strategy to combat the identity fraud problem, establish a central information database of identity fraud incidents, establish a national identity fraud research agenda, as well as more sophisticated domestic and global information sharing networks. In addition, they recommended conducting a study of existing domestic and global policies, laws and regulations to determine the best practices for combating identity fraud. Lastly, they recommended enhancing the protection of individual privacy and information ownership and improve the information and sharing systems that enhance identity authentication solutions while protecting privacy.

This same article by Gordon, Willox, Rebovich, Regan, & Gordon (2004) concluded with the following quote, which best sums up the current status of identity theft:

Identity theft is a growing national and global crisis. Its pervasiveness must be

recognized, especially as a facilitator of crimes that threaten national security, the

economy and global commerce. If identity fraud is not seen as a significant and

insidious threat, it will not be dealt with accordingly. Without a national and

global strategy, identity fraud will continue to grow exponentially, as will the

possibility of financial crimes, terrorist acts, drug trafficking, gun running and alien

smuggling, all of which have an adverse impact on the global community and

commerce. (p. 48)

METHODOLGY

It is the intent of this researcher to show that not only is identity theft the fastest

growing crime in the law enforcement community, but that law enforcement officers are

not properly trained to deal with the problem. Through research into various journals

and publications, this paper will show how identity theft has exploded over the last 20

years, with over 10 million cases reported in 2003, and that the training law enforcement

officers should be receiving regarding this issue, is lacking. For research purposes,

only Texas peace officers, and their training in identity theft, will be addressed. The

author intends to conduct a survey of police departments that represent all geographical

areas of Texas.

Currently, the Texas Commission on Law Enforcement Officer Standards and

Education (TCLEOSE) only requires Texas peace officers to attend 4 hours of training

on identity theft. Based on the complexity, severity and frequent occurrence of identity

theft, as evidenced earlier, 4 hours of training is a very inadequate amount of training to

properly educate a law enforcement officer to effectively investigate an identity theft

crime. The author constructed a survey regarding identity theft training to verify what he believed to be true: that most Texas peace officers have received little or no training beyond what is required by TCLEOSE. The survey posed 6 questions to officers from 17 agencies that were located throughout the state of Texas and were representatives of towns and cities that ranged in size from a couple of thousand residents to one hundred thousand plus. To gain this information, the author asked the participants the following questions: number of sworn officers in their Agency, if there is a problem with identity theft in their community, if they had received training regarding identity theft, other than what is required by TCLEOSE and if so, how many hours, if they had received further training, was it provided by their Agency, or did they seek it themselves and lastly, did the participant feel there is a need for identity theft training. The actual survey can be found at the end of this paper.

As expected, the survey showed that there is a problem with identity theft crimes across the state of Texas. Only 6 out of the 17 surveyed had attended training other than the 4 hours required by TCLEOSE. Of these 6 officers, 5 had attended training provided by their Agency, the other had sought training on their own. Also as expected, 100 percent of the respondents said that they felt that there was a need for more training for law enforcement officers regarding identity theft.

FINDINGS

After researching the definition of identity theft, the author found that almost every paper, article, journal, and website reviewed had their own definition of what identity theft was. Perhaps the best definition found by the author was one from the United States Department of Justice. Identity theft is a crime. It refers to a crime in

which someone wrongfully or illegally obtains another persons personal information and then either uses or sells it to another to be used, in an illegal manner for deception or economic gain. Interestingly, the author also found almost as many ways that identity theft crimes can be committed. But, there is one thing all identity crimes have in common. They all begin with the theft of a person's information that belongs solely to that person. The author found that the ways that this information is stolen can be disturbing, confusing and even amusing.

Naturally, there were some means of identity theft that were obvious. The theft of a wallet or purse, theft of information by an employee at retail locations or businesses that have access to personal information or simply listening to individuals talking to each other about their private business. Some of the more unusual means the author discovered were ones that most people probably do not usually give much attention to. One in particular, dumpster diving, gives true meaning to the old phrase "one man's trash is another man's treasure." Simply put, dumpster diving is someone literally going through garbage looking for information that has been thrown out with the common trash. Often, people will throw away credit card bills, bank statements, utility bills and even pre-approved credit offers without a second thought. However, all of these contain vital information that an identity thief can use to their advantage. Almost all of these contain some kind of account number, address or phone number that a thief can use for illegal purposes.

Another target that is popular to the identity thief is the United States Postal Service. Many times a thief will steal mail directly from a person's mailbox. As with dumpster diving, a thief can often find bank statements and bills that they can use.

Sometimes, they might even get lucky and get an actual credit or debit card. It is also not uncommon for an identity thief to go to the local post office and fill out a change of address form. They can then have a person's mail delivered to the address of their choosing, gain whatever information their after, and then use that information for illegal purposes. They can also take the information gained through these methods and actually call the bank or credit card company and pose as the person whose identity they have stolen. It's not hard for them to do since they have nearly all the information about these accounts at their fingertips.
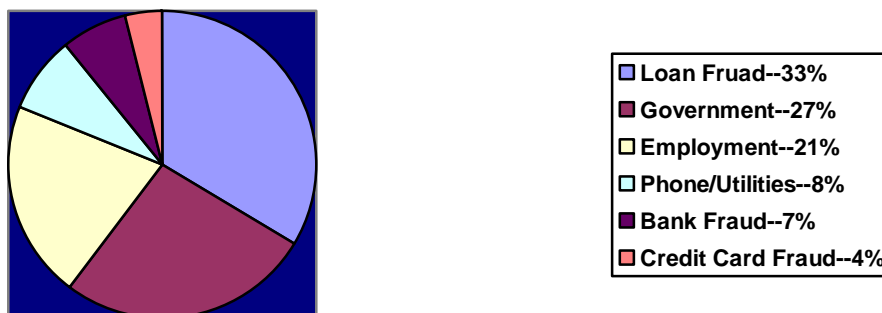
With the invention of the internet and the widespread use of computers, a new form of identity theft has come about in the last 10 years or so. "Phishing" is the term used when a person uses either the telephone or the internet and poses as a legitimate business or representative of a legitimate business and tries to gain personal information from individuals to use in an illegal manner. Along the same lines, identity thieves may employ themselves at businesses that give them access to electronic scanning devices. Since most people either use credit or debit cards, it is easy for someone working at the retail level to steal someone's name and account number. The same goes for writing a check. Nowadays, most checks require a drivers' license number along with a home address and or telephone number. Since the checking account number is printed on the bottom of the check, this one document alone contains enough information for an identity thief to get off to a good start.

The author also found that even though economic gain is the major motivating factor behind identity theft, it is not the only one. Using another person's information for employment is also on the rise. This information is usually used by illegal immigrants,

who could not otherwise get a job or by an individual who, because of their background, does not qualify for they type of job they are seeking. This same information is often commonly used to have utilities turned on, purchase cell phone service or apply for bank loans or credit cards. The following chart shows the breakdown in the percentages of the different types of identity theft crimes.

Figure 1

**Percentages of fraud committed
Due to Identity Theft**

- Loan Fruad--33%
- Government--27%
- Employment--21%
- Phone/Utilities--8%
- Bank Fraud--7%
- Credit Card Fraud--4%

The following chart illustrates the number of identity theft crimes reported, per capita, by state for 2005.

Figure 2

| Top 10 states for identity theft (on per-capita basis)			
Rank	State	Victims/100,000	Total victims
1	Arizona	142.5	8,186
2	Nevada	125.7	2,935
3	California	122.1	43,839
4	Texas	117.6	26,454
5	Colorado	95.8	4,409
6	Florida	92.3	16,062
7	New York	92.0	17,680
8	Washington	91.1	5,654
9	Oregon	87.8	3,156
10	Illinois	87.6	11,138

Based on this information, these 10 states accounted for 139,513 of all cases of identity theft reported in the United States. What the author did not anticipate finding was how high the State of Texas was on this list. Even more surprising, was the fact that Texas would have been second on the list if the list had been based only on cases filed instead of cases filed per capita. However, it did confirm the author's belief that identity theft is a fast rising crime, especially in Texas. What the author also noticed was that several of these states on this list are states that have a high population of retirees. Even though research has shown that 18-29 year olds are the largest group targeted for identity theft, trends have also shown that identity theft crimes committed against the elderly are on the rise.

Concerning law enforcement training and identity theft, the author found that even though there appears to be many avenues of training available to officers, not many are taking advantage of it. Even though this may contribute to the fact that most

identity theft crimes go un-solved, the author found that there were many other factors, most of which could be addressed through training. One of the biggest factors that the author found was the lack of cooperation between the credit industry and law enforcement officials in investigating identity theft cases. Jurisdictional issues and weak security measures were also cited. As part of the research, the author conducted a survey of 17 different police agencies around the State of Texas. 19 officers responded to the survey and all indicated that they had at least attended the required training for identity theft. A few others had indicated additional training, but all indicated that there was a definite need for more training regarding identity theft. The following chart shows the result of this survey. A copy of the actual survey is attached at the end of this research.

Number of officers responding
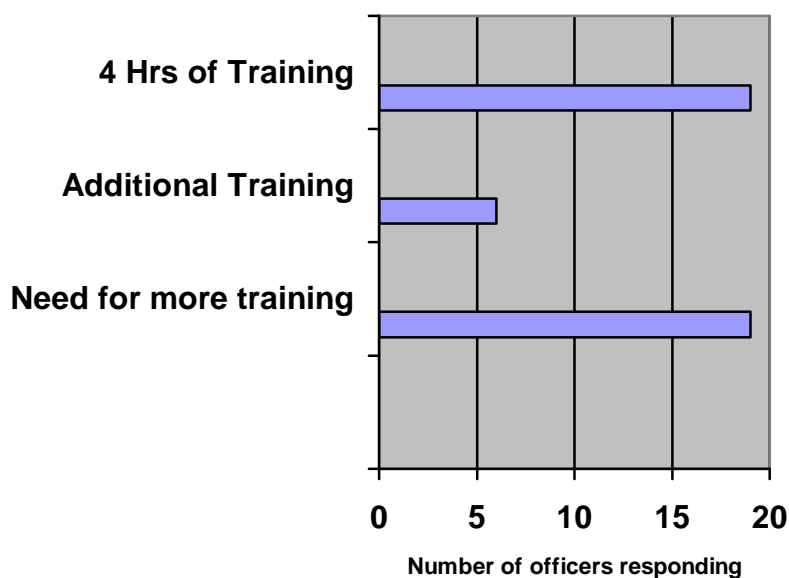
The author also found several steps that should be taken if someone becomes a victim of identity theft that could be useful. Once a theft is discovered, it is

recommended to immediately contact the 3 credit reporting agencies and advise them to flag the account in question. Also, credit card companies and banks should be called and told of the theft. This is very important as it will protect the consumer from any illegal charges or accounts that have been opened as a result of identity theft. Naturally, a police report should also be made. Irregardless of whether or not a person has been a victim of identity theft, it is recommended that at least once a year, people get a copy of their credit reports to verify that the information contained in them is correct.

CONCLUSIONS

The purpose of this research was to determine if identity theft was indeed a fast growing problem. It was also the intention of the author to establish the problems that victims of identity theft face as a result of having their identities stolen. Through the various articles and journals reviewed by the author, the original statement that identity theft is fast growing, was proven. Identity theft was found to be the fastest growing problem facing law enforcement today. The number of identity theft cases reported each year has reached into the millions, world wide. No one age group is safe from this threat, from 18 to 80 being victims.

The various means in which identity theft occurs is almost as numerous as it's victims. From simple methods such as the theft of a checkbook or credit card, to complicated schemes involving scams over the phone or computers. There is virtually no information that is completely personal and private anymore. As technology becomes smarter, so do identity thieves. However, no matter what new security measures are implemented, it is just a matter of time before identity thieves are able to

overcome them. Ironically, it is becoming more difficult for victims of identity theft to clear their names and credit reports.

The training currently provided to law enforcement officers is not at the level it should be. The training opportunities are there, but not many agencies are taking advantage of them and providing their officers with the training that could benefit them. Even with the cooperation difficulties and lax security that was cited from various credit companies, law enforcement agencies could greatly benefit from the training that is currently available. The results of the survey supported the original idea that not only is the current amount of training inadequate, but that officers feel that there is a need for more training regarding identity theft crimes.

Before the author began to investigate this particular topic, there was little doubt as to whether there would be a problem in finding information on the subject. On the contrary, the amount of information available on identity theft is almost overwhelming. When it comes to this subject, you could find out anything from how it happens, how to prevent it, prosecute it or even commit it. The author took the standpoint on identifying what identity theft is, identifying ways in which it occurs, the training available to law enforcement officers and general information on what steps to take should it occur. Most information contained in this report was obtained from various journals and articles as well as information derived from the internet, for which there were literally thousands of websites on the subject.

The topic of identity theft was chosen for research for one, simple purpose. To provide the reader with an insight into the problem in which this crime poses on our society. By showing the seriousness and ease of this crime, it is the author's hope that

the reader will become aware of what to look for to deter identity theft from happening to them. At the same time, the author wanted to show the lack of training for law enforcement and the difficulty they often have in solving identity theft crimes. It was not the author's intention to show that officers have difficulty because the crime itself is complex, but that most agencies do not have the manpower or resources available to properly train officers to investigate identity theft.

REFERENCES

Dadisho, E. (2005, January). Identity theft and the police response: The problem.

    Police Chief, 72(1), 25-29.

Federal Trade Commission. (2006). *Take charge: Fighting back against identity theft.*

    (Federal Trade Commission). Washington D.C.

Gordon, G., Willox Jr., Rebovich D., Regan T., & Gordon J. (2004). Identity fraud: A

    critical national and global threat. *Journal of Economic Crime Management, Utica*

    College.

Newman, G. (2004). *Identity Theft (25). Problem-specific guides for police.*

    U.S. Department of Justice, Office of Community Oriented Policing Services.

    Washington D.C.

Pavlicek, B. (2005, July/August). Identity theft and SLIT rings: An unrecognized yet

    growing cancer. *Crime & Justice International,* 29-33*.*

Pinheiro, R. (2004). Preventing identity theft using trusted authentications. *Journal*

    of Economic Crime Management, 2(1), 1-16.

United States Department of Justice (2006). *What are identity theft and identity.*

    fraud? (Fraud Section, Criminal Division, U.S. Department of Justice)

    Washington D.C.