The Bill Blackwood
Law Enforcement Management Institute of Texas

"Identity Theft"
Law Enforcements Response

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

By
Vernon T. Tucker

Farmers Branch Police Department
Farmers Branch, Texas
January 2007

ABSTRACT

Identity theft is being called the fastest growing crime in the United States and law enforcement gets poor ratings when it comes to reporting and investigating identity theft. Many police agencies are not aware of the Texas law and Attorney General opinions that dictate law enforcement's response. Twenty small police agencies were surveyed to obtain their understanding and procedures as they relate to the reporting and investigations of identity theft.

Law enforcement response is inconsistent. Some law enforcement agencies refuse to take reports unless it is absolutely clear that the criminal offense offered within their city limits, many times sending the victim to other agencies to file a report that then find themselves in a endless loop of law enforcement agencies referring them somewhere else. Law enforcement must take action, be it an information report or criminal offense report, regardless of jurisdictional issues. Law enforcement needs to explore the possibility of the creation of a multi-jurisdictional task force whose sole responsibility is the investigation and prosecution of identity theft suspects.

TABLE OF CONTENTS

Page

Abstract

Introduction 1

Review of Literature 2

Methodology 4

Findings 5

Discussions/Conclusions 8

References 10

INTRODUCTION

Identity theft has become a problem of epidemic proportions for law enforcement officers today. The number of reported cases continues to increase rapidly, and local law enforcement must take action. The Federal Trade Commission (FTC) has become the nations clearing house for identity theft, their web site (www.consumer.gov/idtheft) is a portal for victims of identity theft as well as law enforcement officials investigating identity theft.

The (FTC)'s, identity theft victim complaint database currently contains more than 815,000 complaints. According to the FTC's September 2003 survey, the personal cost accumulated by victims of identity theft totals approximately $5 billion annually, with the average cost ranging between $500 and $1200 per victim. In addition to the problems of workloads common to all criminal cases, identity theft cases present unique complications of jurisdiction, solvability, etc.

Municipal law enforcement agencies are overwhelmed by the number of criminal cases reported to them and frustrated by their inability to investigate them all fully. In many cases, this frustration stems from the insufficient number of detectives employed by the agency, which leaves each detective with an unmanageable number of criminal cases to be investigated. Those who supervise the criminal investigation divisions must review these cases to determine which cases merit being assigned to a detective. Among other factors, they must consider solvability (are there suspects, witness, physical evidence etc.) Many cases are automatically labeled as "inactive" and filed away until some evidence or additional information is brought up.

Identity theft has compounded this dilemma exponentially. Identity theft investigations can become very complicated and time consuming for a detective, the first objective and often the most difficult is locating the origin (location where offense occurred) and the date of the offense. Many times the original offense occurred several months or even a year prior to the victim realizing that they are a victim of identity theft.

Law enforcement investigation is very territorial, in that offenses have clearly occurred at a specific place and time. Identity theft, however, differs from most cases in that it knows no jurisdictional boundaries. It could take place anywhere in the world, regardless of the victim's residential address. This uncertainty raises a jurisdictional question for law enforcement: where did the offense occur? Who has jurisdiction? Who will investigate?

The author's hypothesis is that to investigate identity theft comprehensively you must establish a specialized unit or dedicated detective, whose sole task is to investigate identity theft. Through research of published articles, interviews and surveys it will be discovered that agencies that do not already adhere to this hypothesis are not investigating identity theft but rather they are only reporting identity theft.

It is the intention of this author to bring to the attention of those agencies who are not effectively investigating identity theft and perhaps encourage further research and collaboration amongst agencies for the betterment of their communities and the law enforcement profession as a whole.

REVIEW OF LITERATURE

According to the (Federal Trade Commission) FTC the 1990's spawned a new variety of crooks called identity thieves. Their stock in trade is your everyday transactions, which usually reveal bits of your personal information, your bank and

credit card account numbers; your income; your Social Security number; or your name, address and phone numbers. An identity thief obtains some piece of your sensitive information and uses it without your knowledge to commit fraud or theft.

The best available estimates to the extent and distribution of identity theft are provided by the FTC from its victimization surveys and from its database of consumer complaints. The most recent estimate, produced by a study modeled after the FTC's original 2003 methodology, suggests that some form of identity theft had victimized 9.3 million adults in 2004 (BBB, 2005).

The Privacy Rights Clearinghouse, a non-profit group in San Diego, Ca., estimates that the identity of 100 million people have been compromised since February 2006. Identity theft has been labeled “the fastest growing crime in America” It is predicted that in the United States alone, 15 million people or 1 in 20 people will have their identity compromised in 2006.

A large number of individual victims do incur financial costs, even though it is commonly assumed that businesses will bear the burden of the financial damage. One study found that the average out-of-pocket expenses reported by victims were between $30 and $2,000, but this estimate does not included any lawyer’s fees that were incurred. The average loss to victims in this study was $808 dollars, but most people estimate spending around $100 (Benner et. al, 2000).

Individuals suffer various types of additional “costs” as a result of their victimization: “human” costs include the time and effort required to resolve various problems created by the theft, the emotional impact or feeling of “violation” that often results, and the frustration of being harassed by debt collectors or dealing with various agencies in trying to resolve problems, “opportunity costs” include the victim’s inability to

obtain a job, purchase a car, or qualify for various types of loans, and the loss of their job – all of which may translate into additional financial costs.

No single federal agency has jurisdiction over cases of identity theft. Many federal agencies are involved in efforts to combat this problem. Since 2002, the Secret Service was the lead agency in 38 different national task forces related to financial or electronic crimes, which often contain identity theft-related elements; however, none of the 38 task forces focus exclusively on the problem of identity theft. One identity theft-related investigation, led by the electronic crimes task force of the Secret Service's New York Field Office in cooperation with the New York Police Department, discovered a group of perpetrators who had obtained (through the use of the internet and cellular telephones) and fraudulently used the credit card account information of some of the wealthiest chief executive officers in the nation, in addition to various other citizens. This group had further attempted to transfer almost $22 million from victims' legitimate brokerage and corporate accounts (GAO, 2002a).

METHODOLGY

Identity theft is a major issue facing law enforcement. The number of cases being reported has created an identified need for specialized units to investigate these crimes. Since Identity theft appeared in the late 1990's law enforcement has fallen behind in its efforts to stop it. Many agencies are still unclear on ways to deal with Identity theft and the understanding of who investigates the crime.

The researcher will review books and articles whose topics include: Identity theft, Cyber Crime, Mail Fraud, and Bank Fraud. Also, the author has read many special reports to Congress and reports to other Governmental entities. During the author's

research, numerous questionnaires will be submitted to Texas law enforcement agencies. The author will also conduct several telephone interviews.

FINDINGS

Texas Municipal Law Enforcement reports Identity theft as, defined by Texas Penal Code statute 32.51, "*Fraudulent Use/Possession of identifying Information".* However, it is not always a clear-cut case of Identity theft and there may be jurisdictional issues and in many instances officer(s) file a Information Report which is not reportable to the State or Federal data collection systems instead of an offense report.

A number of governmental agencies do not maintain separate statistics related to identity theft. Many of the agencies reporting to the (Governmental Accounting Office) GAO, therefore, provide estimates based on while-collar crime or other categories of financial crimes. A majority of these estimates were not directly related to costs, but to arrests, investigations or prosecutions. It can generally be assumed that higher rates of criminal justice outcomes will translate into higher criminal justice operating costs, although such data does not present an accurate picture of the identity theft-related costs incurred by the government.

Local law enforcement takes the brunt of criticism because it does not responded to the individual victims of identity theft. Local law enforcement places a band-aid on the problem by giving the victim a "police report" for their documentation. Local law enforcement perceives the problem as not one that they, the police, should be dealing with. It was, after all, the credit card issuing companies and banks that were taking the bulk of the financial loss. Furthermore, retail stores, banks and individual cardholders, seldom report offenses to the police. According to the FTC, only 26 percent of victims

report the incident to the police. It is also common for banks and retailers to decline to report offenses to the police because of built in *losses*. The financial institutions determine it to be a cost of doing business. The visibility of police on their property sends the signal of "something's wrong" and is potentially bad for business.

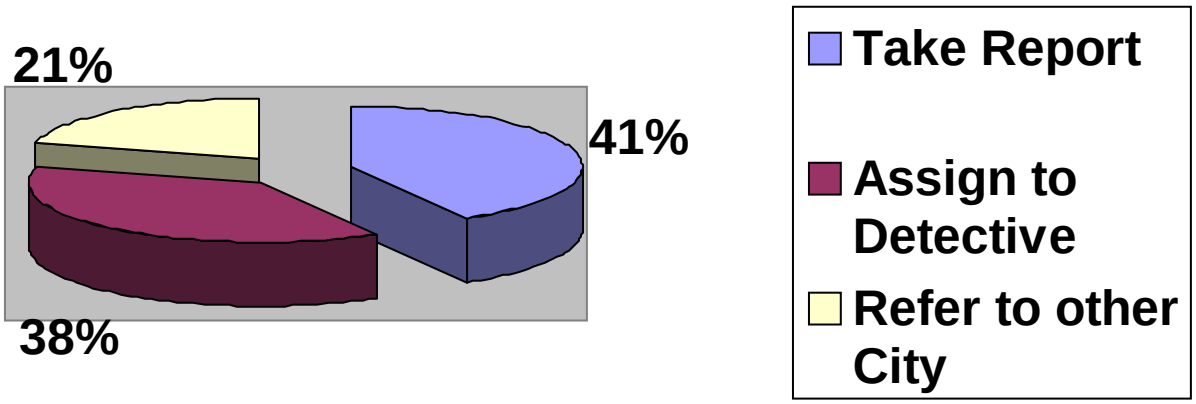
Victims of Identity theft many often feel victimized twice, once by the thief and once by law enforcement. They feel that they are getting the runaround by law enforcement. Initially, and in some instances – still the case, police departments were not set up to record these types of crime since it is a crime that in the course of its commission may span several jurisdictions. A victim's credit card may be stolen in Texas and used in Arkansas or on the Internet to make purchases that are then shipped to California. So who has jurisdiction and who should record the offense? In 1998 the FTC was tasked with being the nations clearinghouse for Identity theft. However, they don't investigate the crime. The FTC assists victims of Identity theft with avenues of clearing their good name, but plays not part in investigating the crime, tracking down the suspect or prosecution of the offender. Due to the many reports to Congress, legislation was passed that requires credit-reporting agencies to respond quickly to victims of Identity theft and provide the victim with assistance in clearing their credit. This has increased the number of individuals reporting the crime to police, since they are required by credit reporting agencies to submit an Identity theft Affidavit, which requires a police report. The Texas Attorney General, Greg Abbott, has ruled that every Texas law enforcement agency, to which a person wishes to report Identity theft, must take a written report and provide that person with a report number. In addition, The (International Association of Chiefs of Police) IACP, (2000) and many other law enforcement groups have passed resolutions urging police departments to provide

police reports for identity theft victims. The IACP has further urged that the rule to be followed is that the police department in the jurisdiction in which the victim lives should take responsibility for issuing the report.

Law enforcement agencies are compelled to follow the Texas Attorney Generals Opinion; however, some smaller jurisdictions are not aware of this ruling and either refuse to take a offense report or at best file an information report, giving the victim a report number and sending them on their way without the intention of doing any type of investigation or follow-up.

Twenty surveys were sent out and twenty surveys were completed. The data confirms that law enforcement agencies are not handling Identity theft cases the same way. Only 44 percent of agencies surveyed stated that they would take a offense report regardless of jurisdictional issues. However, only 39 percent of these agencies would assign the report to a Detective for investigation. 21 percent of the law enforcement agencies would not take a report, referring the victim to the law enforcement agency where the Identity theft was believed to have occurred.

Survey Results



Twenty-four Texas law enforcement agencies were surveyed targeting small agencies, the average size ranged from 16 to 440 police officers. The returned surveys indicate that none of the agencies had detectives assigned to work only identity theft. Ten of the surveyed agencies indicated that they would take a report regardless of jurisdiction, none agencies would assign the report to a detective and five agencies would not take a report and refer the victim to another agency.

CONCLUSIONS

Identity theft continues to be a burden on law enforcement nation wide. Research indicates that every State in the United States, with few exceptions, has Identity theft statutes. Each of the States provide adequate information to their Citizenry on how to prevent Identity theft, obtaining assistance in reporting their claim, and clearing their credit. Yet, they all come short in the investigation, arrest and prosecution

of offenders. Locally, some of the larger law enforcement agencies have dedicated detectives assigned to Identity theft or Financial Crimes Units where Identity theft falls under their umbrella. The majority of agencies, particularly small agencies find them-self struggling to keep up with case filings and prosecutions of other “high-profile” cases and do not have the luxury of time in order to properly investigate Identity theft. Smaller law enforcement agencies neither have the financial or departmental support to actively investigate Identity theft, nor try to stop Identity theft from occurring.

Local law enforcement continues to take the brunt of criticism because it has not responded to the individual victims of identity theft. The police often perceived the problem as not one that they, the police, should be dealing with, but rather a Federal issue. The Federal Government has the financial and human resources to effectively investigate these offences that do not recognize jurisdictional borders. Often times the Federal response is that the “loss value” does not meet it’s monetary threshold to justify an investigation thereby placing the responsibility back on local law enforcement.

Identity theft investigation continues to evolve. Efforts to resolve this issue will undoubtedly will be debated for years to come. In the mean time local law enforcement must commit resources to help combat this epidemic. If efforts are not made law enforcement will no longer be effective in investigating and prosecuting offenders, they will continue to be a reporting portal for individuals to clear their good name and a way of obtaining statistical data for State and Federal Agencies, leaving the financial industry to fend for themselves – ultimately absorbing the loss.

REFERENCES

Benner,J., Mierzwinski E., & Givens, B. (2000, May). *Nowhere to turn: Victims speak out on identity theft*. California Public Interest Research Group and the Privacy Rights Clearinghouse. Retrieved January 24, 2006, from http://www.calpirg.org/consumer/privacy/idtheft2000/idtheft2000.pdf

Federal Trade Commission. (2005). *Take charge: Fighting back against identity theft* Washington, DC.: U.S. Government Printing Office

Federal Trade Commission, (2003). *ID theft: When good things happen to your good name.* Washington DC.: U.S. Government Printing Office.

Hearing before the Special Committee on Aging United States Senate, (2002, July). *Identity Theft: The nation's fastest growing crime wave hits seniors.* Washington, DC.: U.S. Government Printing Office.

Hearing before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and The Census, (2004, September). *Identity theft: The causes, cost, consequences, and potential solutions.* Washington, DC.: U.S. Government Printing Office.

Morris, R.G., II. (n.d.). *The development of an identity theft offender typology: A theoretical approach*. Retrieved January 15, 2006, from http://www.shsu.edu/~edu_elc/journal/research%20online/re2004/Robert.pdf

NCJRS, National Criminal Justice Reference Service. Retrieve January 15, 2006, from http://www.ncjrs.gov/spotlight/identity_theft/programs.html

Newman, G. (2003). *Check and card fraud.* Problem oriented guides for police No. 21. Washington, D.C.: Dept. of Justice, COPS and center for problem oriented Policing. Retrieved January 15, 2006, from http://www.popcenter.org/Problems/problem-check-card-fraud.htm.

Newman, G. (2004a). *Identity theft*. Problem oriented guides for police No. 25. Dep. of Justice, COPS and center for problem oriented policing. Retrieved January 15, 2006, from http://www.popcenter.org/Problems/problem-identity_theft.htm

Office of the Inspector General, (1999, May). *Using social security numbers to commit fraud*. Management Advisory Report [A-08-99-42002]. Retrieved January 15, 2006, from http://www.ssa.gov/oig/ADOBEPDF/auditpdf/ad99-4~1.pdf

Star Systems, (2001, December). *Identity theft in the United sates: an update.*

Branigan, S. (2004). *High-tech crimes revealed.* Boston: Pearson Education, Inc.

U.S. General Accounting Office, (2002c, March). *Identity theft: Prevalence and cost appear to be growing*. Report to Congressional requesters. Washington, D.C. [GAO-02- 363] http://www.gao.gov/new.items/d02363.pdf

U.S. General Accounting Office, (2002d, February 14). *Identity theft: Available data indicate growth in prevalence and cost*. Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate, [GAO-02-424T]. Retrieved January 15, 2006, from http://www.gao.gov/new.items/d02424t.pdf