Identity Theft Investigations: An Analysis of Challenges that Law Enforcement Faces in Conducting Investigations and Suggestions for Improvement in the Process

Approved: Susan Hilal Date: July 21, 2009
Advisor

Identity Theft Investigations: An Analysis of Challenges that Law Enforcement Faces in Conducting Investigations and Suggestions for Improvement in the Process

A Seminar Paper

Presented to the Graduate Faculty

University of Wisconsin-Platteville

In Partial Fulfillment

Of the Requirement for the Degree

Master of Science in Criminal Justice

By

Angela Pretasky

2009

Acknowledgements

My thanks go out to all who assisted me in so many different ways in the completion of this degree and this paper. I attribute much of my success to the following people.

First, I thank my colleagues who have been with me throughout this Masters program. Your support, feedback, and individual input made this an enjoyable journey and a wonderful learning experience.

Second, I thank my criminal justice professors for showing me how fulfilling the field of criminal justice really is. A special thanks to Dr. Randall Beger from the University of Wisconsin Eau Claire for the guidance in helping me obtain my first job with probation and parole and the encouragement I needed to continue my education after completion of a Bachelors Degree.

Lastly, I thank my family. This specifically includes my mom, Debra Pretasky, my dad, Chris Pretasky, and my sister, Lisa Pretasky. You all have been with me throughout my entire educational career. Your help and support could not be more appreciated.

This paper is dedicated to all those who have been victims of identity theft. Be reassured that law enforcement is aware of the problem and steps are being taken to combat this growing crime.

Abstract

Identity Theft Investigations: An Analysis of Challenges that Law Enforcement Faces in Conducting Investigations and Suggestions for Improvement in the Process

Angela Pretasky

Under the Supervision of Dr. Susan Hilal

Statement of the Problem

Currently there is an inadequate system in place to track and investigate identity theft. There are numerous obstacles that make investigating and reporting identity theft difficult, thus making it problematic to determine the actual magnitude of the problem confronting the criminal justice system. First, no criminal justice agency oversees all identity theft cases, and no single database exists to record relevant information (McNally & Newman, 2007). Second, identity theft may be a combination of several crimes, making recording and distinguishing the crime as identity theft difficult. Third, one of the greatest hurdles that make investigating identity theft difficult is a single offender using several identities or aliases (Roberson, 2008). Fourth, confusion arises on whose responsibility it is to investigate the case when one offender may be victimizing someone in another city, state, or even country. The fifth barrier that makes investigating identity theft difficult is many victims do not report their crimes to law enforcement authorities.

Methods and Procedures

Secondary research and statistics are used to illustrate the lack of an accurate recording and reporting system for managing identity theft crimes. Data gathered from scholarly journals, newspaper articles, books, the Bureau of Justice Statistics, and the National Institute of Justice is used to illustrate the nature of this problem and to examine methods to correct the problem. Reviews of empirical literature on the recommendations that have been made by researchers to

address the problem are discussed in detail. Conclusions and suggestions on how to track identity theft and how managing systems could be improved are offered based on the collective information presented in this paper. The arguments are based on the notion that the current methods of managing identity theft are ineffective.

Summary of Results

The evidence collected in this study supports that the current process for tracking and prosecuting identity thieves needs to be restructured, more coordinated, and better organized. In order to arrest and prosecute identity thieves, an effective law enforcement response is critical. An effective response includes cooperation from police departments, financial agencies, and identity theft victims. It goes without saying that crimes not reported to police usually go unsolved. Therefore, any bank, credit card issuing agency, financial agency, individual, etc. should be required to report all identity theft cases to police. Further, it should be mandatory for investigating officers to enter identity theft profiles into a single database. Computerized case management systems have proven successful in tracking various other crimes and should be implemented in identity theft cases.

Table of Contents

SECTION I: INTRODUCTION

Introduction:

Identity theft has become one of the fastest growing problems in the United States and throughout the entire world. It is commonly thought of as a crime involving stolen personal credit cards or social security numbers, but it is now becoming a larger threat to governments and corporations worldwide (Wagner, 2007). It is a crime that affects individuals and businesses in every community ranging from small towns to major cities. Although individualized acts of identity theft still occur, the crime is happening more frequently on a larger scale. As more and more information is available electronically, the potential and opportunity for committing the crime is growing. In December of 2004, the Federal Deposit Insurance Corporation (FDIC) released a study regarding online identity theft. The study revealed that in the year 2004, almost 2 million adults experienced some type of identity fraud, many of whom pay their bills and do their banking online (FDIC, 2004). The study also found that an estimated 19% of electronic bill paying services have experienced some type of hacking/fraud (FDIC, 2004). Acts of identity theft cost the U.S. economy billions of dollars every year. The challenge is for law enforcement to find an appropriate way to protect the integrity of personal information and to hold perpetrators criminally responsible for their crimes.

Identity theft is not a violent offense, but the consequences to victims and businesses can be devastating. An effective law enforcement response is critical in order to successfully arrest and prosecute identity thieves. Maintaining an accurate reporting system for identity theft cases would provide data on the true extent of this crime. Knowing the true enormity of identity theft would be a motivating factor for law enforcement and governmental agencies to implement safeguards against being victimized and to implement methods at combating the crime.

However, there are numerous barriers that make investigating and reporting identity theft difficult, thus making it problematic to determine the actual magnitude of cases confronting the criminal justice system.

Statement of the Problem:

Law enforcement officers face a number of obstacles when investigating and tracking identity theft. First, no criminal justice agency oversees all identity theft cases, and no single database exists to record relevant information (McNally & Newman, 2007). Therefore, police officers are not trained to systematically record this type of information, and it is not currently mandatory that investigating officers enter identity theft profiles into a single database. Although police officers do use police reports to record cases of identity theft, the information on the reports is not systematically entered into an organized database. Information on identity theft can be found in a number of different places which make investigations by police departments hard to carry out.

Second, identity theft may be a combination of several crimes, making recording and distinguishing the crime as identity theft difficult. For example, offenders may hack into a victim's computer, obtain personal financial information, and use that information to make a fraudulent purchase on a credit card. This links the crimes of hacking, theft and credit card fraud in one single act and may not be treated as an identity theft case. Police departments lack effective ways to record identity theft cases as separate crimes. For example, the theft and use of a credit card may be prosecuted as credit-card fraud and theft without indicating that identity theft was ever involved (Roberson, 2008).

Third, one of the greatest hurdles that make investigating identity theft difficult is a single offender using several identities or aliases (Roberson, 2008). Identity thieves can use home

computers to look up information about a person, apply for a credit card, or request confidential information anonymously by using several identities in the midst of committing one fraudulent crime (Britt, 2009). When an offender uses a false identity or alias, investigators do not even have an accurate suspect with which to start their investigation. This causes great perplexity among investigators trying to track one identity thief.

Fourth, confusion arises on whose responsibility it is to investigate the case when one offender may be using technology to victimize someone in another city, state, or even country. Jurisdictional boundaries complicate investigation efforts since one case may span several jurisdictions (McNally & Newman, 2007). Identity theft can originate just as easily from a neighboring city as it can from across the globe. For example, a Spanish criminal could steal the identity of an American citizen and use it to defraud a Mexican bank. Language barriers can further complicate investigations that take place over a variety of jurisdictions or a variety of countries. Even when an identity thief is prosecuted, getting a victim to testify at a trial out of state is difficult. In April of 2007, the Executive Summary of the Presidents Identity Theft Task Force reported that law enforcement officers faced many challenges because of multi-jurisdictional investigations and a severe lack of resources with the proper skill sets (Roberson, 2008). There is a lack of a collaborative effort on the parts of national and international governments, the private sector, and industry to combat identity theft.

The fifth barrier that makes investigating identity theft difficult is many victims do not report their crimes to law enforcement authorities. Individuals are more likely to report their victimization to their banks, credit card companies, or other financial institutions rather than the police (McNally & Newman, 2007). Most financial institutions have loss prevention departments that handle and dispose of cases and write off the financial loss as a result of doing

business. In circumstances like those, one case of identity theft has two victims: the financial institution that pays for the monetary loss and the individual whose identity was stolen. Financial institutions are routinely defrauded by identity related crimes and the fraud is never reported to law enforcement. As a result, even if there were a single database to record identity crimes, law enforcement may not even know the crime happened. The burden of these types of cases should be placed on police departments rather than on banks, credit card companies, or other financial institutions.

It is clear that the existing systems for tracking and investigating identity theft are inefficient. The current process needs to be restructured, better coordinated and more organized. Identity theft is costing individuals and businesses billions of dollars each year and is becoming one of the fastest growing financial crimes in America, but there is not an effective system in place to combat the crime. Without an accurate reporting and recording system in place, more and more cases of identity theft will occur and offenders will continue to successfully carry out crimes with no repercussions. Individuals and businesses will continue to be victimized and will continue to suffer the losses. Although no one solution exists to prevent identity theft and no two cases are exactly the same, improvements can be made to enhance the investigation process.

Purpose of the Research:

The purpose of this research is threefold. Initially, it will demonstrate that current methods of tracking and investigating identity theft crimes are inadequate, ineffective, and inefficient. Secondly, it will provide an in depth discussion of the current recommendations that have been made by academic researchers and adopted by government agencies on how to better monitor and record identity theft. Lastly, a conclusion will propose recommendations to the current tracking system so the criminal justice system will be better equipped to handle this

growing crime. Specifically, law enforcement needs to develop and maintain a national database for recording cases of identity theft. Although national databases already exist to record various other types of crimes, no national database currently exists to record all identity theft cases. Additionally, law enforcement, financial institutions, and individual citizens should be mandated to report all cases of identity theft so relevant information can be entered into the national database. Currently, it is not mandatory for citizens or police officers to report identity theft cases to a single agency, causing complications in investigating and tracking this crime. This research will focus on ways to realistically fix the current and inadequate methods of tracking and recording identity theft.

Significance and Implications of the Research:

This research is particularly significant during this time of a failing economy because identity theft is one of the fastest growing financial crimes worldwide (Cameron, 2008). Individual identities have always been vulnerable to identity theft, but advances in technology have made it easier to obtain private information, significantly increasing the opportunities for crime (Roberson, 2008). Experts and law enforcement officials who track internet crime say fraudulent acts have multiplied in the past year as scammers attempt to take advantage of economic failure and collapse (McQueen, 2009). A recent report warns the Obama administration that identity theft is about to explode due to a dismal economy, fewer resources for law enforcement, and budget constraints that make police departments focus on public safety rather than protecting personal information (Britt, 2009).

This research paper is an informational resource for law enforcement investigators and is intended to assist in educating local, state, and federal agencies to develop methods to better secure people and business' personal information. It provides an in depth discussion on ways to

overcome the various challenges law enforcement officers currently face when handling identity theft cases. It is anticipated that by developing measures to counteract those challenges, a larger number of offenders will be prosecuted and a smaller number of individuals will be victimized.

Limitations of the Research:

Since a majority of victims do not report their victimization to law enforcement, a serious lack of statistical data is available on identity theft, and the data that is available may not accurately portray the true nature of the problem (McNally & Newman, 2007). Numerous studies have unsuccessfully attempted to measure the actual extent of the crime (Roberson, 2008). Further, few studies have been done evaluating effective programs or policies in place to reduce identity theft. The limitations in the amount of empirical data make research into possible intervention strategies very difficult to develop.

Method of Approach:

Secondary research and statistics are used to illustrate the lack of an accurate recording and reporting system for managing identity theft crimes. Data has been gathered from scholarly journals, newspaper articles, books, the Bureau of Justice Statistics, and the National Institute of Justice to illustrate the nature of this problem and to examine methods to correct the problem. Reviews of empirical literature on the recommendations that have been made by researchers to address the problem are discussed in detail. Conclusions and suggestions on how to track identity theft and how managing systems could be improved are offered based on the collective information presented in this paper. The arguments are based on the notion that the current methods of managing identity theft are ineffective.

SCETION II: REVIEW OF THE LITERATURE

Introduction:

Identity theft has been prevalent for some time and many definitions have been adopted over the years, but there is confusion on what officially constitutes a case of identity theft. The one thing that is apparent is no one is immune from being the victim of identity theft. It can happen to anyone, any time, and at any place. That being the case, the government has enacted legislation to help control the crime, and there are a number of prevention strategies that have been developed so people can better protect themselves from being victimized. Specialized training is also needed for law enforcement to better identify and dispose of identity theft cases and to keep up with technologically advanced crimes. The following section provides information on the definition of identity theft, the scope of the problem, underreporting of this crime, the various crime reporting systems currently used, current legislation regarding identity theft, ways to safeguard against becoming a victim, and specialized training designed for police officers and investigators working on identity theft cases.

Definition of Identity Theft:

The most common definition of identity theft that is used was drafted in 1998 by the Federal Identity Theft Assumption and Deterrence Act. It states that identity theft is the act of "knowingly transferring or using, without lawful authority, a means of identification of another person with the intent to commit, aid, or abet any unlawful activity that constitutes a violation of federal law or constitutes a felony under any state or local law" (as cited in Heller, 2007, p.84). Identity theft is a crime in which an imposter obtains key pieces of personal information and uses them for their own personal gain. First, the thief illegitimately obtains key pieces of the victim's

personal information and second, uses that information as his/her own and benefits from the gains, while the victim is left to suffer the losses.

An identity thief can use stolen personal information such as a name, social security number, date of birth, passport number, address or driver's license number for personal and/or monetary gains. Identity theft includes almost any situation where a person uses another person's personal information for his or her own benefit. The crime can be as simple as making a purchase on someone else's credit card or as complicated as being arrested under a false identity or alias. Some common examples of identity theft include using a friend's identification when stopped by police, medical personnel using patient's information to open new credit card accounts, terrorists using false visas and passport numbers and obtaining another's bank account information to withdrawal money.

It is important to note that not all identity theft involves a financial loss. Any crime committed to fraudulently obtain or use another's personal information is associated with identity theft. Some examples of common ways thieves commit identity theft without involving a financial loss are through lost or stolen wallets, misappropriation from family and friends, and through paper mail and e-mail containing personal information (Gana, 2007). Victim's personal information is also used to obtain fraudulent government documents like passports and tax forms.

The definition of the term identity theft is not agreed upon by everyone. Law enforcement working at all levels subscribe to the definition of knowingly using the identification of another person with the intent to commit unlawful activity. However, the financial services industry disagrees and tends to classify the fraudulent use of stolen credit card numbers as "payment card fraud" rather than identity theft. This distinction and the different

views on what constitutes a crime of identity theft held by the general public, the government, the private business sector and the financial community complicates investigations collaborative efforts.

It is imperative to examine the different typologies of identity theft in order to understand the effect they have on criminal investigations. Currently, there are two distinctive typologies of identity theft. The two typologies include financial gain and concealment (Roberson, 2008). Financial gain refers to identity theft committed with the intent to secure a monetary gain. Concealment refers to identity theft committed to assume the identity of another with the purpose of covering up one's true identity.

Each typology is further distinguished based on the level of organization and commitment the thief has in carrying out the crime. Offenders with high organization and commitment are usually professionals who put a significant amount of planning into the crime they commit, causing large numbers of people to become victims (Roberson, 2008). An example is a fraud ring that systematically steals personal information from customers by luring them into unauthorized websites. Offenders with low commitment and organization commit identity theft crimes at the spur of a moment when an opportunity presents itself. There is little planning and organization involved and the crime is committed to solve an immediate problem. An example of a low commitment identity theft crime is using false identification when pulled over for a traffic stop.

Scope of the Problem:

The Federal Trade Commission (FTC) has estimated that nearly 10 million Americans become victims of identity theft each year, costing businesses and consumers roughly $47.6 billion (FTC, 2006). The Identity Fraud Survey Report released in February of 2009 by Javelin

Strategy and Research confirmed that the number of identity fraud victims has increased 22% since 2005 in the United States (Sovern, 2009). A Government Accountability Office (GAO) report found that identity theft allegations reported to Social Security Administration grew five-fold from 1998 to 2001 (GAO, 2002). The FBI's statistics on bank fraud arrests with identity theft being a substantial component rose from 579 in 1998 to 645 in 2000 (GAO, 2002). No follow up studies have been conducted by GAO to determine if this number has continued to grow since 2000. The FTC estimates the average loss to a victim is about $371, but about ½ of victims do not know how someone obtained their personal information (FTC, 2008).

It is certain that businesses and consumers alike suffer from acts of identity theft. In the year 2000, MasterCard and Visa sustained about $1 billion loss to identity theft/payment card fraud (GAO, 2002). In many cases, businesses accept this type of loss as part of doing business and do not pursue criminal charges. Therefore, the actual cost of identity theft to businesses is generally unknown (Roberson, 2008). What is known is that all consumers suffer from these types of losses since consumers have to pay higher prices for businesses to offset the losses sustained. There is no doubt that individuals as well as businesses suffer financially from identity theft, but also suffer from frustration, disappointment and a loss of time after being victimized.

In 2003, the FTC conducted a study regarding identity theft and the impact it had on victims. The study was conducted via telephone from a random group of 4,000 U.S. adults who had been the victims of some form of identity theft within the last five years. The survey found that the mean amount of fraud a victim experienced was $5,720, and victims spent an average of 40 hours trying to resolve the crime and their losses (FTC, 2003). After a victim finds out his or her identity has been stolen, it takes a considerable amount of time to resolve the issue with

banks, credit card companies, and other interested parties. This study found that the emotional impact on victims was parallel to the negative impact experienced from victims of violent crime (FTC, 2003). Victims often receive innumerable phone calls or letters from creditors wanting information. Being that many of these crimes are so complicated, it is taking victims longer and longer to straighten out their finances and personal identification with institutions.

In 2003, the Identity Theft Resource Center conducted a study on 173 known victims of identity theft. The study found that only 15% of victims found out about their identity theft through proactive measures taken by financial institutions (FTC, 2003). The other 85% found out about it in negative ways like receiving an expensive credit card bill (FTC, 2003). A follow up study on victims of identity theft was conducted in 2005 and found that a slightly larger number of victims (20%) found out about their identity theft through proactive measures taken by financial institutions (FTC, 2006). Statistically, this shows that constructive measures are being taken to reduce identity theft incidents.

The devastating effects this crime can have on consumers and businesses are motivation to ensure that justice is brought for those that commit the crime. However, the number of cases that actually make it to court are few and far between. District attorney's offices have cutoff levels for acceptance of cases based on financial loss, time for discovery, and involvement of an organized group (McNally & Newman, 2007). It was estimated that the FBI and U.S. Secret Service processed a few thousand cases of identity theft in 2004 (McNally & Newman, 2007). Assuming that a similar number of cases were processed in every state and in various task forces, this would yield an estimate of about 303,000 processed cases, leaving over 9.5 million cases a year that never make it to the criminal justice system (McNally & Newman, 2007). Offenders are aware that the odds of getting caught are slim, creating little to no deterrence from

committing the crime. In order for deterrence to be effective, punishment should be certain, swift, and severe (Beccaria, 1963).

The above statistics are a good start to determining the magnitude of this crime, but the current methods of quantifying identity theft are inadequate due to the inefficient system put in place to track, record and quantify this crime. There have been numerous studies conducted by federal agencies to measure the number of identity theft cases confronted by police, but the data only provides an estimate of the true extent of the crime. Numerous governmental organizations have conducted unsuccessful studies attempting to measure the cost and significance of this crime. There is considerable debate about the true extent and cost of identity theft, but everyone agrees that billions of dollars are spent each year recovering the losses occurred from identity theft (Roberson, 2008). The studies conducted are producing incomplete data as a result of the inefficient system in place to record and quantify this crime and to the underreporting of identity theft cases.

Underreporting of Identity Theft Cases

Compared to visible street crime, identity theft crimes are vastly underreported. There are a few explanations for why many cases of identity theft go unreported to police. One explanation is that investigators face challenges of overcoming information sharing between law enforcement and the private sector. Many financial institutions consciously decide to not report the case to police nor share any offense details to protect their consumer's personal information (Owens, 2004). Therefore, if the victim solely reports the victimization to their financial institution and not to the police, the crime goes unreported. Investigators have encountered difficulties obtaining such information from financial institutions without a subpoena. Even when companies are presented with warrants for a search, some financial companies will not

accept warrants from another state (Owens, 2004). They choose to accept the monetary loss as a consequence of doing business and not get involved with law enforcement. They claim concern for customers over liability which causes a major roadblock for law enforcement and slows or even stops the investigation process (Owens, 2004).

A second explanation for the underreporting of identity theft cases is due to the physical distance and multiple jurisdictions between perpetrator and victim. This poses additional problems for investigators. A detective in New York City could be attempting to trace a perpetrator in Los Angeles who stole the identity of a business group of victims in New York, Miami, Dallas, and Chicago. At the very least, evidence will need to be traced through all of these jurisdictions. These types of investigations require the coordination and efforts of numerous agencies requiring time, resources and a considerable amount of money. This scenario gets even more complicated when the suspect is located outside the United States. Coordination of tracking one identity theft scheme can be both extraordinarily complicated and cost prohibitive.

A third explanation for the underreporting of identity theft cases is due to the lack of a specific definition. Identity theft crimes may be reported to law enforcement but may be recorded and handled as cases of fraud or theft instead of identity theft. Police departments do not have proper technology to cross reference cases of fraud and theft that also involve stolen identities.

Underreporting is significant because law enforcement resources are allocated based upon the number of reported crimes. Rapes, murders, robberies, and assault related offenses are of higher priority than identity theft crimes because of their violent nature. Underreporting has added to the many issues detectives face during identity theft investigations and has sparked

interest among various agencies to develop task forces aimed at preventing identity theft. Although underreporting is a common issue in identity theft cases, crime reporting systems are currently available to record data that does come to the attention of law enforcement.

Crime Reporting Systems:

In the United States, there are two main systems of collecting and reporting data on crimes committed. The first is the Uniform Crime Report (UCR). The UCR system only collects data from crimes that come to the attention of law enforcement. Law enforcement could be notified through victim reports or public observation. As with cases of identity theft, it is a known fact much crime in this country goes unreported to law enforcement. Therefore, all the unreported crime is not accounted for in the UCR. In many identity theft cases, victims report their crimes to their financial institution who accept the loss as part of doing business and no further action in the case is taken. These types of crimes are not accounted for in the UCR. Further, the UCR does not contain a separate category for recording cases of identity theft nor does it do a thorough job of tracking white collar crime. However, another common crime reporting system, the National Incident Based Reporting System (NIBRS), does address some white collar statistics. The NIBRS contains data on each reported crime incident and goes into much greater detail on the crimes than the UCR. Like the UCR, the NIBRS does not contain a separate category for recording identity theft. It does, however, contain a category for recording cases of fraud including offenses like impersonation, credit card fraud, and wire fraud.

The third system of collecting and reporting data on crimes committed is through the National Crime Victimization Survey (NCVS). The NCVS takes into account crimes reported to law enforcement *and* crimes not reported to law enforcement. Twice each year, data is obtained from a cross section of the community comprised of a random sample of households. People

have the opportunity to report crime on this survey that they may not have reported to police. Therefore, the NCVS may have record of the crime while the UCR may not. This causes a numerical difference in the data reported by the UCR and the NCVS and could cause significantly different results.

An adequate solution to acquiring accurate statistics on identity theft is creating a national database to record relevant information and mandate that law enforcement and financial institutions report all cases of identity theft. The current system in place to track and investigate identity theft is not advanced enough to address the complexity of the crimes and overcome the numerous obstacles law enforcement officers face when attempting to quantify cases. Mandatory reporting and entering of identity theft data would alleviate the inconsistent data currently available. Because identity theft investigations are labor intensive and generally require a staff of detectives, agents, and analysts with multiple skill sets, increased resources must be devoted to them to ensure accurate investigations while still protecting individual privacy (Gonzales, 2007). Using a national database to record true identity theft cases has the potential to produce more valid statistics on identity theft cases.

Current Laws:

Government has been challenged to enact effective state and federal legislation to protect personal information and hold offender's accountable for identity theft crimes. The Federal Government and most states have passed legislation to impose criminal sanctions on identity thieves (McNally & Newman, 2007). As identity theft cases have become more prevalent and more sophisticated, laws and policies have been developed and implemented to combat this crime. However, it has been proven that prosecuting identity thieves is time consuming and complicated. A study conducted in 2007 by the Identity Theft Resource Center found that only 1

in 700 identity thieves are successfully apprehended and an even smaller number are successfully prosecuted (Heller, 2007).

Currently, there is one primary federal criminal law used against identity thieves called the Identity Theft and Assumption Deterrence Act. This Act makes it illegal to knowingly use someone else's identification as one's own with the intent to commit a crime. Violations of this act are punishable by up to 25 years in prison (Roberson, 2008). This act was created with the intention of making the law applicable to a wide range of conduct that may be prosecuted as identity theft (Roberson, 2008). This legislation extended protection to anyone whose personal identification was misused, causing a loss or suffering (Roberson, 2008). Losses can be monetary or nonmonetary. Since this act was created in 1998, similar legislation has been developed addressing identity theft crimes.

Although the Identity Theft and Assumption Deterrence Act is the primary federal criminal law used against identity thieves, it is not the only federal law in place to control the crime. Some current federal legislation currently used in identity theft cases are the Aggravated Identity Theft Act, Computer Fraud and Abuse Act, Fair Credit Reporting Act, Credit Card Fraud Act, USA Patriot Act, and Drivers Privacy Protection Act. This is only the start of an extensive list of federal legislation available relating to identity theft, but has prompted state and local levels to start taking actions.

Identity theft is also addressed in state legislation. Each state is responsible for developing and implementing their own laws regarding cases of identity theft. In every state except Maine, identity theft can be a felony depending on the severity of the crime (Foster, 2008). For example, Alabama has enacted a law requiring credit reporting agencies to block false information that shows up on victim's credit reports (Heller, 2007). Rhode Island has

passed a law stating that no person shall require consumers to disclose social security numbers when purchasing goods or services (Heller, 2007). All state and federal legislation has been designed to prevent and deter criminal acts involving stolen identities. Depending on the nature of the crime, the offender could be charged with fraud, identity theft, theft, fraudulent misinterpretation, credit card fraud, misappropriation of identifying information, impersonation, and even harassment. Each charge holds a different maximum penalty.

Although federal and state legislation has been enacted to counter this crime, recent reports indicate that the government is not currently taking extra measures to keep confidential information safe from identity thieves. A 2008 Consumer Report investigation showed that government is one of the biggest sources of identity leaks, and penalties are rarely imposed on those who are negligent (Foster, 2008). For example, Ohio resident Joe Protain got a traffic ticket for $150, and the traffic court records posted the ticket information, his name, address, and social security number on the municipal county website allowing identity thieves to obtain his information and rack up $11,427 worth of fraudulent charges under his identity (Foster, 2008). Protain's penalty for speeding was far greater than the $150 as his identity information was sold to fraudsters and subsequently used all over the country to open new credit cards and make fraudulent purchases. A GAO study conducted in 2004 found that up to 28% of counties publicly displayed citizen's social security numbers and other personal information on the internet (as cited in Foster, 2008). Breaches of information make committing an identity theft crime reasonably simplistic to carry out. The Center for Identity Management and Information Protection at Utica College completed a study in October of 2006 regarding identity fraud. They found that breaches of confidential information from the internet, businesses, medical records, employers, and private corporations make identity theft difficult to track (Choo, Gordon, &

Rebovich, 2007). In response, defense mechanisms have been recommended to consumers to help protect their personal information.

Although identity theft has been a federal offense since 1998, there are concerns that the criminal justice system has failed in dealing with this growing crime. A study conducted from a municipal police department in Florida found that the number of incidents of identity theft appeared to be growing at a greater rate than other theft related offenses, but the clearance rate was declining (Allison, Schuck, & Lersch, 2005). Legislation has been passed and a number of government based recommendations have been developed to deter people from committing identity theft. However, due to the rapid advances in the field of technology, identity theft has become a seemingly simplistic crime to carry out but extremely difficult to track, investigate, and prevent.

Ways to Safeguard Against Identity Theft:

The general public is vulnerable, but also uncertain, of how to safeguard against identity theft. There are a number of ways individuals can protect themselves from becoming victims of identity theft. It is important for consumers to look for signs that indicate victimization. Some indications include receiving credit card bills for cards that belong to someone else, receiving calls or letters about unknown purchases, or having a credit card application get denied due to bad credit when the line of credit should be good. Some of the most plausible ways to defend against being a victim of identity theft are safeguarding social security numbers, avoid providing personal information to anyone through e-mail, not sharing computer passwords, using firewall protection on computers, shredding personal documents, and protecting credit card numbers.

Special programs have been set up to assist individuals in protecting their personal information and avoid becoming the victim of identity theft. One such program is called

Lifelock. Lifelock is a personal fraud protection company that works to safeguard customer's personal information. For a fee of $10 per month, Lifelock works with credit bureaus to run credit fraud alerts, remove names from pre-approved credit card offers, order credit reports, and assist in lost and stolen wallet issues (Lifelock, 2006). It is important to limit breaches in confidential information so fraudsters do not have easy access to personal information. Lifelock is one particular program that takes proactive measures to protect their customer's personal information (Lifelock, 2006). It is essential that private citizens, government, law enforcement and industry work together to keep personal information confidential to cut down on acts of identity theft. It takes the cooperation of all individuals and agencies to safeguard breaches of confidential information.

Specialized Training:

The crime of identity theft is exploding, creating a need for qualified technology specialists who oversee programs to safeguard information. According to an FBI report, online criminals cost U.S. organizations $11.9 billion per year (as cited in Nishi, 2007). The $11.9 billion figure does not take into account the time, energy, and sense of security that is also lost in identity theft crimes. The majority of police officers are unprepared to deal with technologically advanced crimes (Harrison, Heuston, Mocas, Morrissey & Richardson, 2004). Most police academies do not train personnel in such involved investigation techniques (Harrison, et al., 2004). The result is a lack of proper skill sets for law enforcement officers which complicate investigations.

Training police officers to investigate computer crimes is expensive and challenging. A properly trained computer crime investigator may require extensive ongoing professional education to maintain up-to-date skills (Dadisho, 2005). Because computer companies introduce

new software products frequently, staying ahead of the learning curve is a monumental task. Since no single investigator can know every system, a number of officers must be trained to specialize in a variety of programs (Dadisho, 2005). There is also the considerable cost of the highly specialized computer equipment to consider. The challenges facing police in their attempts to keep up with hackers who scheme to commit identity theft crimes are daunting (Dadisho, 2005).

As society has become more computerized, people have witnessed an increase in high tech crimes including online identity theft and online hacking of personal information (Harrison, et all., 2004). The police are not properly trained to manage such complicated systems nor are they trained to investigate technologically advanced crimes, such as identity theft. In most circumstances, police officers are not the computers experts within the agency. Some police departments hire qualified individuals with degrees in Computer Forensics or Information Technology, and some departments may hire qualified analysts to decipher recovered information. Being that more jobs are available for highly qualified computer specialists, there has been a growth in the number of programs at colleges and universities in areas like computer forensics. Combining efforts between police officers and computer specialists help agencies overcome some of the difficulties in investigating technologically advanced crimes.

The International Association of Chiefs of Police (IACP) recommends that police officers be educated on the latest technology to recognize possible identity thefts during routine traffic stops and other detentions (IACP, 2005). Some signs that officers have been trained to look for are possession of blank checks, various credit cards, laminating machines, involvement in computer crimes, and money laundering (Roberson, 2008). A police department's first step in combating this crime is to ensure that officers have sufficient knowledge of what identity theft is,

who commits it, and how it is committed. They also recommend that a standard procedure for handling identity theft cases be developed and new officers should be trained to use it (IACP, 2005). Consistency in handling cases will assist in more accurate investigations and more correct information available on the case. The IACP acknowledges that identity theft is a crime and when incidents are reported, they should be investigated as fully as would any other crime.

The Federal Trade Commission has expanded their recommendations for a successful investigation process and has encouraged that law enforcement agencies educate citizens on identity theft warning signs (Roberson, 2008). Victims should be encouraged to file police reports on any suspected identity theft crimes. The police should then be mandated to report the crimes to a single criminal justice agency who would record relevant information into a single database. The more information available to the police, the easier it will be to track the perpetrator.

Conclusion:

It is clear that identity theft is a growing problem in society today. Although initiatives have been taken to legally penalize those who commit the crime, the number of victims is still growing. The current crime reporting systems available to do accurately account for the true number of identity theft cases and do not take into account the high number of underreported cases. Cooperative efforts from law enforcement and financial agencies are necessary to combat this crime.

SECTION III: COOPERATIVE EFFORTS

Introduction:

Despite numerous efforts on the part of law enforcement, citizens, and private companies to combat identity theft, there has been little cooperation and coordination between agencies resulting in an inefficient system to control identity theft. Since the private sector and financial institutions are such an important source of identity theft-related information, the President's Identity Theft Task Force recommended that the private sector and law enforcement find a means to fully cooperate with each other. It is clear that identity theft is a complex problem involving several entities. Federal law enforcement agencies recognize the importance of cooperation among agencies and coordination of information sharing between law enforcement and the private sector (Gonzales, 2007). This coordination has been difficult for several reasons: identity theft data is in numerous databases; there is no standard reporting form for all identity theft complaints; and many law enforcement agencies have limited resources (Gonzales, 2007). With no standard system for disposing of identity theft cases, confusion arises and many cases are lost within the system. This section will briefly discuss the various task forces that have been created to combat identity theft, the success that single reporting systems have had in the criminal justice system, and the success of mandatory reporting of cases.

Separate Task Forces:

Law enforcement has responded to the challenge for greater cooperation by forming interagency task forces designed to improve the sharing of information. According to the United States Department of Justice (DOJ), the following federal authorities lead or co-lead a total of 96 task forces and working groups devoted to identity theft (DOJ, 2006). Some of those task forces include:

Federal Trade Commission (FTC): The FTC provides support for criminal law enforcement through its Identity Theft Clearinghouse, which is the national compilation of consumer complaint data (DOJ, 2006). The Federal Trade Commission's Identity Theft Clearinghouse is the current repository for identity theft complaints. All local, state, and federal law enforcement officers have free internet access to this secure database (Roberson, 2008). Law enforcers across the country use this secure online resource of more than one million complaints to identify trends and targets. However, not all complaints are entered into this site due to a lack of a standard procedure in handling identity theft cases. Although this is a good start to systematically managing cases, the database does not contain information on suspects or criminal investigations. This resource encourages greater coordination and data sharing among the more than 1,300 law enforcement agencies that have access to the system (DOJ, 2006).

US Attorney's Office: US Attorney's offices lead 27 identity theft task forces and work groups across the country to participate in identity theft tracking (DOJ, 2006). The Presidential Task Force recommended that United States attorneys designate an identity theft coordinator for each U.S. attorney's office and establish an identity theft program for each district (Roberson, 2008). Similar coordinators are also recommended for local prosecutors' offices. It would seem that there is an extensive network of court personnel assigned to the investigative process. However, it must be considered that the sheer size and scope of this task force initiative complicates efforts to function efficiently.

Federal Bureau of Investigation (FBI): The FBI leads 4 task forces and participates in 21 task forces in most of the major metropolitan areas. In addition, the FBI's Cyber Division has more than 90 task forces and more than 80 work groups consisting of federal, state, and local law

enforcement personnel, which investigate all cybercrime violations including identity theft and internet fraud (DOJ, 2006).

Secret Service: The Secret Service has 27 financial crimes task forces and 24 electronic crimes task forces that focus on identity theft related crimes (DOJ, 2006).

Postal Inspection Service: The Postal Inspection Service actively leads 13 financial crimes task forces across the country (DOJ, 2006).

Immigration and Customs Enforcement (ICE): Immigration and Customs Enforcement has established document and benefit fraud task forces in 11 cities nationwide to enhance interagency communication and improve each agency's effectiveness in fraud investigations (DOJ, 2006).

The Financial Crimes Enforcement Network (FinCEN): FinCEN is a network that currently exists to investigate identity theft and other financial crimes. FinCEN links databases maintained by law enforcement, financial, and business corporations to collect, analyze, and share information (Dadisho, 2005). They access approximately 37 different databases to obtain information (Dadisho, 2005).

Various task forces have also been created at the state and local level to combat identity theft. For example, Alabama has created a task force designed to develop a cooperative effort between federal, state, and local law enforcement agencies challenged with the investigation and prosecution of identity theft and related offenses (Cameron, 2008). Pennsylvania created a task force in 1995 to assist law enforcement in investigating, arresting, and prosecuting individuals committing financial crimes and identity theft (Cameron, 2008). These types of task forces have been established at the federal, state, and local level.

Reporting Systems:

Investigators certainly have numerous sources where reported identity theft data is stored, but it is virtually impossible to check every single database in every single investigation. Using a single database to better organize this information could simplify investigation efforts. The recommendation of a national data base that tracks all identity theft profiles has the potential to improve collaboration efforts from all the various agencies working on identity theft cases. Developing a nationwide, computerized management system for recording cases of identity theft would cut back on the many jurisdictional issues associated with this crime. All jurisdictions and task forces need access to the same database for recording and investigating cases.

Critics worry that it will take only one person with the right access to the national database that is careless or corrupt, and the whole country's records will become vulnerable (Cameron, 2008). Ross Anderson, professor of Security Engineering at Cambridge University and one of the government's most heated critics, argues that local systems are far more secure than national ones, and gigantic databases only place citizen's privacy and safety at risk (Cameron, 2008). To keep possible breaches of personal information to a minimum, a developed national database should contain only pertinent information. A single criminal justice agency, namely law enforcement investigators, need to be designated to handle all identity theft cases so the information stored in the database is not accessible to private individuals, financial institutions, or other government entities without legitimate permission. That single agency could then enter relevant information into a single system, like the UCR or NIBRS, to provide information in aggregate regarding statistics related to identity theft.

The use of a single database to systematically record crime related information is not new. In 1967, the National Crime Information Center (NCIC) was established and continues to operate today (Aftergood, 2008). The NCIC is a computerized index of criminal justice

information including criminal histories, fugitives, stolen property, and missing persons (Aftergood, 2008). It is available to local, state, and federal law enforcement agencies nationwide and is accessible 24 hours per day, but the information is protected from unauthorized individuals. Using the National Crime Information Center as a central information database would create a sophisticated domestic and global way to share information, thus making identity theft investigations easier to carry out (Choo, Gordon, & Rebovich, 2007). The downfall in the NCIC is that not all crimes are recorded in the system, identity theft being one of those crimes.

The Center for Identity Theft Management and Information Protection at Utica College conducted a study of identity theft in 2004. They partnered with LexisNexis, IBM, the US Secret Service and the FBI to supply research on trends in identity theft fraud and ways to combat it. Among their recommendations on ways law enforcement could more effectively combat identity theft fraud was the need to establish a central information database of identity fraud incidents (Choo, et al., 2007). Further, the Presidential Identity Theft Task Force recommended creating a national identity theft center to help law enforcement agencies coordinate efforts to investigate and prosecute identity thieves (Roberson, 2008).

The recommendation that it should be mandatory for investigating officers to enter identity theft profiles into a single database is partly based on the success that computerized management systems have had on investigating other crimes. In 2008, a study of homicide units was conducted across the United States. A questionnaire was prepared that pertained to a variety of operational and management issues and focused on how successful homicide units investigate homicide cases. The police departments chosen for the study included only departments with 25 or more homicides per year over a five year period and only departments that submit crime data

to the Uniform Crime Report Program (Keel, 2008). Eighty-one departments received questionnaires and 55 completed and returned them. Collected data revealed that 64% of all responding departments had a computerized case management system for their homicide unit, with 62% sharing the information with other criminal investigation units (Keel, 2008). The study found that police departments with a computerized case management system had a 5% higher clearance rate of homicide cases than departments that did not have a computerized case management system (Keel, 2008).

The computerized database enhanced investigations with potential leads because information was recorded in a systematic and organized way. This study shows that having a computerized case management system increased the rate of clearance of homicide crimes. If it is true for homicide investigations, it can be reasoned that it would be true for identity theft investigations as well. Fortunately, a lot more people fall victim to identity theft than homicide, but the idea behind the computerized case management system in clearing cases is the same. Critics of this argument pose that a computerized case management system works for homicide cases due to the low number of cases entered. If a similar system were developed for identity theft cases, the database would need to be able to handle the large volume of cases. The development and maintenance of a national database would require specialized training for those in charge of operating the system to ensure information accuracy and protection.

The recommendation that it should be mandatory for investigating officers to enter identity theft profiles into a single database is also based on the success that single recording systems have had on prosecutions involving the use of DNA. Currently, it is mandatory for all felons to submit a DNA sample, and all samples are stored in a national DNA database. When detectives are investigating crimes and collect DNA, the information is run through a computer

system (Moore, 2009). A positive match in DNA gives detectives a place to start with their investigation. In the same respect, identity theft cases could be entered into a single database so information collected could be cross referenced with information already entered. In cases where DNA is tested, a single investigation could involve many people including patrol officers, detectives and volunteer workers (Moore, 2009). Since they are all referencing the same DNA database, collaborative efforts are easier to carry out. Since 1989, using a single DNA database for recording DNA has played an important role in thousands of criminal convictions (Moore, 2009). Along with using a single recording system for DNA profiles, federal, state, and local agencies use the same method for entering and comparing fingerprints. The Automated Fingerprint Identification System (AFIS) is a computerized system used to store fingerprint data, electronic images, and criminal history information (AFIS, 2008). These types of automated systems are being implemented to solve crimes all over the country and are producing favorable results. By using a single database to store DNA profiles and fingerprints, investigators are solving some of the most unimaginable crimes.

The use of a single database has proven successful in combating various other crimes. One recent example is the implementation of a technologically advanced database to track and investigate insurance fraud. Within the insurance field, a single database has been developed and is known as the National Insurance Crime Bureau (NICB). It is used to store and consolidate insurance industry claims so investigators can check for repetitions in claims and uncover possible fraudulent activities (NICB, 2000). The use of the NICB has allowed for the development of software that can cross reference claims and help investigators uncover fraudulent activity. The use of a consolidated database has aided investigators in prosecuting individuals involved in insurance fraud (NICB, 2000). However, even with the use of a

database, it is imperative that these types of cases are reported to law enforcement or no action will be taken.

Success of Mandatory Reporting of Crime:

Another one of the most reoccurring topics in tracking identity theft is the recommendation for the mandatory reporting of identity theft cases to law enforcement, requiring cooperation from all those involved. In the same way it is mandatory to report cases of child abuse, it should be mandatory for businesses and financial institutions to report cases of identity theft. The Federal Trade Commission conducted a study in 2003 among identity theft victims. The study found that only 25% of victims who participated in the study reported their crime to police (Roberson, 2008). Police are not able to track and prosecute identity thieves if they are not made aware that the crime took place. The study also recommended the establishment of a more sophisticated domestic and global information sharing network requiring active participation from all those involved in the process (Choo, Gordon, & Rebovich, 2007).

In 2003, a study was conducted by the Public Interest Research Group in Michigan (PIRGIM) with 22 law enforcement officials across Michigan who regularly investigated identity theft cases. In-depth interviews were held focusing on personal experience with identity theft crime. The study revealed that identity theft investigations are problematic because credit card companies, banks, etc. will not provide police departments with the information they need, such as copies of checks or falsified applications (Owens, 2004). Many financial institutions just do not care about the losses and do not want to become involved in the investigation process. Due to the evidence collected from PIRGIM, recommendations were made for consumers and companies on ways to slow identity theft, track the crime, and prosecute thieves. They developed a policy recommendation that would require companies to give criminal investigators

evidence in a timely manner (Owens, 2004). Officers involved in the PIRGIM study commented that they also work on many other cases so a more organized and efficient system would decrease the amount of time needed to clear an identity theft case (Owens, 2004).

Steps have been taken to get the community actively involved in reporting identity theft cases to the police. The Federal Trade Commission has conducted a national public awareness campaign using the theme "Deter, Detect, and Defend" to help prevent identity theft (Roberson, 2008). The campaign encourages individuals to monitor their credit reports and credit card accounts to alert themselves of any possible issue and immediately turn suspicious information over to police. Victims of identity theft are the main source of information during investigations since they hold the financial records that the investigator may need, such as a list of possible suspects with access to their information. Therefore, victim's cases should be treated seriously and appropriate action should be taken in all cases. For these reasons, all victims are encouraged to report their crimes to police.

The May 2006 Executive Order stated "it shall be the policy of the United States to use its resources effectively to address identity theft, including increased aggressive law enforcement actions designed to prevent, investigate, and prosecute identity theft crimes, recover the proceeds of such crimes, and ensure just and effective punishment of those who perpetrate identity theft" (as cited in Majoras, 2006, p.2). The question becomes what is the effective method of carrying out that order. Those working on solving identity theft cases need to implement strategies that have proven successful in combating various other crimes. Reasoning suggests that similar strategies will produce similar favorable results in clearing cases. The findings from this research regarding identity theft crimes support the recommendation for a single database

containing all identity theft case information and the mandatory reporting of identity theft cases requiring cooperation from all agencies.

Cooperation between Agencies:

Cooperation between many agencies in tracking identity thieves has proven successful in the past. One of the country's biggest identity fraud-heists ever prosecuted happened in Boston and San Diego in 2008. Defendants located in Miami engaged in a sophisticated scheme involving "sniffer" programs that allowed them to gain access to credit card numbers that consumers were swiping at major retail stores, store them in an encrypted computer software program, and sell the numbers to people in Latvia and Ukraine (Pereira, Levitz, & Singer-Vine, 2008). The defendants extracted tens of millions of dollars from people's bank accounts across the country and from major retail chains like TJ Maxx and Marshall's (Pereira, et al., 2008). Due to the fact that three suspects were from the United States, two from China, one from Estonia, and another from Belarus, investigating the case became more challenging as new evidence started pouring in. Solving the case eventually involved the collaboration of computer security experts, the Department of Justice, the Secret Service, attorneys, and police departments from the United States, Turkey, Germany, Ukraine and Estonia (Pereira, et al., 2008). Without the continued cooperation of all these agencies, the identity thieves would have continued using the identities stolen from "sniffer" programs and more individuals and businesses would have fallen victim to this ring of identity thieves.

It is essential that law enforcement take advantage of all resources available in tracking and investigation identity crimes, especially in technologically advanced crimes. Cooperation in tracking identity theft has not only existed between various agencies, but by citizens as well. For example, the Hillsboro, Oregon Police Department set up a program called the Police Reserve

Specialist Program (PRS). The program allows suitably qualified individuals from the community to assist the police department with investigating internet related crimes and provides a pool of expertise where police chronically lag behind criminals (Harrison, Heuston, Mocas, Morrissey, & Richardson, 2004). The program brings a sense of community policing into action and is beneficial for both the program volunteers and the police department. An evaluation of this program concluded that the program has produced positive results in solving crimes, and there should be no reason the program could not be duplicated elsewhere (Harrison, et al., 2004). Cooperation between investigators, police officers, and computer savvy citizens has the potential to combat identity theft crimes across the spectrum. Cooperative efforts will reduce the problems associated with investigating identity theft (Dadisho, 2005).

Cooperation from many agencies has proven successful in detecting and deterring various other types of crimes. For example, a study was conducted by the Government Accountability Office (GAO) in 2007-2008 regarding the selling and purchasing of defense-related property. The investigation was started after a 2005 GAO report found that an excess of defense-related property had been lost, stolen, or damaged, and numerous items were found on two online store websites. Data was collected by undercover investigators who went onto Craigslist and eBay to determine how easy it was to obtain these types of items. Investigators worked with cooperating agencies including eBay's Fraud Investigations Team to obtain info about the identity of the sellers, the Department of Defense to see if the sellers were active military members, Defense Criminal Investigative Service, Demilitarization Coding Management Office, Air Force Office of Special Investigations, and the Army of Criminal Investigation Division (GAO, 2008). They also collaborated with Department of Defense to find out exactly what items were "defense-related." Due to the cooperation of all these agencies, the GAO was able to track down

individuals who were illegally selling and purchasing defense related items and refer proper cases to the police (GAO, 2008).

Conclusion:

It is clear that identity theft is a complex problem involving several entities. However, state and federal agencies have taken active steps at developing legislation, creating safeguards for consumers, and preparing police departments to handle complex computer crimes. It is essential that victims report crimes to police and that police enter that information into a single system. The use of single systems has proven effective in storing DNA and fingerprints and could also be effective in storing information on identity theft. Although it is true that identity theft is not a violent offense, victims are falling more prone to this crime every day. Local, state, and federal levels of government need to take active steps to counter this crime and implement methods that have been proven to work in combating other crimes.

SECTION IV: RECOMMENDATIONS and CONCLUSION

Introduction:

With a proper tracking and investigation system in place, identity theft is a crime that can be prevented if proper safeguards are implemented. Crime victims, law enforcement, businesses and prosecutors all have a role in preventing identity theft crimes from occurring. The following section makes two key recommendations on ways to improve the current investigation process of identity theft cases based on the researched gathered in this paper. The two recommendations include the need for a single, national database to record all cases of identity theft and the mandatory reporting of identity theft cases, requiring cooperation from all those involved in a case.

Need for a National Database:

Currently, a national database containing all information related to identity theft does not exist. However, numerous agencies have agreed that creating a national database would be an efficient way to track and record cases. As part of their strategic plan to combat identity theft, the Task Force recommends that a national identity theft law enforcement center be created for agencies to better coordinate efforts and to effectively investigate cases (Gana, 2007). A single criminal justice agency should oversee a national database that contains all identity theft case information. Although there are positives and negatives in doing this, findings support that it should be mandatory that investigating officers enter identity theft profiles into a single database, conceivably the National Crime Information Center (NCIC), making information available to law enforcement nationwide. The NCIC is available to record crime data and information. Using the National Crime Information Center as a central information database has created a sophisticated domestic and global way to share information, making identity theft investigations

easier to carry out (Choo, et.al, 2007). It would be logical to use this system for identity theft crimes, along with all the other crimes that are entered into the system.

Investigators have numerous sources where reported identity theft data is stored, but it is virtually impossible to check every single database in every single investigation. A single database would improve the current system in place for law enforcement's response to identity theft. This recommendation has been made by a variety of government based agencies and should be implemented to strengthen the current tracking system. A central database would allow law enforcement to quickly analyze, share and coordinate information across a number of jurisdictions.

Jurisdictional boundaries complicate investigation efforts since one case may span several jurisdictions (McNally & Newman, 2007). Identity thieves usually leave behind a trail of evidence but that information is usually spread across multiple jurisdictions and rarely assembled into one concrete case. A national database would allow the trail of evidence to be pieced together during an investigation. It would give law enforcement the necessary tool to stay ahead of the savvy criminals. Developing this type of system would also enable researchers to present more accurate statistics on the true extent of this problem. Statistics on the nature of the problem may make investigation efforts more common and make committing this crime less attractive.

As recent studies have shown, the use of a single database has proven successful in combating other crimes. A study of homicide units across the nation revealed that 64% of all responding departments had a computerized case management system for their homicide unit, with 62% sharing the information with other criminal investigation units (Keel, 2008). The study found that police departments with a computerized case management system had a 5% higher clearance rate of homicide cases than departments that did not have a computerized case

management system (Keel, 2008). Being that identify theft is a relatively recent phenomenon, strategies to combat the crime need to be based on what has been proven to work in the past with other crimes until new methods are developed specifically for identity theft.

The use of a single database has also proven successful in storing and matching DNA samples and fingerprints. Since 1989, using a single DNA database for recording DNA and a single database for entering and comparing fingerprints has played an important role in thousands of criminal convictions (Moore, 2009). These types of automated systems are being implemented to solve crimes all over the country and are producing favorable results (AFIS, 2008). It is important for law enforcement officers and prosecutors to look at the success rates that these single databases have played in the convictions of thousands of offenders when implanting strategies to combat identity theft.

A national database may also help investigators cross reference details from more than one offense to solve a crime. For example, offenders may hack into a victim's computer, obtain personal financial information, and use that information to make a fraudulent purchase on a credit card. This links the crimes of hacking, theft and credit card fraud in one single act and may not be treated as an identity theft case. Identity thieves can use home computers to look up information about a person, apply for a credit card, or request confidential information anonymously by using several identities in the midst of committing one fraudulent crime (Britt, 2009). A single database containing all relevant information may be able to connect these crimes and give investigators the tools necessary to solve a case.

Due to the rapid advances in the field of technology, identity theft has become widespread and extremely difficult to track, investigate, and prevent. In order to arrest and prosecute identity thieves, an effective law enforcement response is critical. Developing a

nationwide, computerized management system for recording cases of identity theft would cut back on the many jurisdictional issues associated with this crime. All jurisdictions need access to the same database for recording and investigating cases. Developing a single database is one step towards achieving this goal as well as preventing and detecting identity theft.

Mandatory Reporting of Identity Theft Requiring Cooperation From all Agencies:

Another reoccurring recommendation to help track and investigate identity theft cases is that any bank, credit card issuing agency, financial agency, individual, etc. should be required to report all identity theft cases to police, not just their financial institution. Currently, there is no federal law requiring a federal agency to take a report about identity theft and systematically record it, but some state laws require local police departments to take reports (Owen, 2004). It is recommended that current legislation change to require all federal, state, and local police departments to file a completed police report on identity theft cases and enter relevant information in the national database.

Federal law enforcement agencies recognize the importance of cooperation among agencies and coordination of information sharing between law enforcement and the private sector (Gonzales, 2007). The Presidential Identity Theft Task Force has affirmed the need for a fully coordinated approach to fighting this crime, requiring cooperation from all those involved (Roberson, 2008). Due to the 2003 PIRGIM study, a policy recommendation was developed that would require companies to give criminal investigators evidence in a timely manner to create a more organized and efficient system and decrease the amount of time needed to clear an identity theft case (Owens, 2004). Cooperation is needed in response to the many daunting obstacles law enforcement officers face in conducting investigations, such as multi-jurisdictional issues and the use of aliases.

Police officers are not trained to systematically record case information, and it is not currently mandatory that investigating officers enter identity theft profiles into a single database. Further, individuals are more likely to report their victimization to their banks, credit card companies, or other financial institutions rather than the police (McNally & Newman, 2007). When crimes are not reported and recorded, they cannot be solved. There is an extensive network of agencies (Unites States Secret Service, the Federal Bureau of Investigation, the United States Postal Inspection Service, the National Criminal Intelligence Resource Center, U.S. attorney's offices, U.S. Immigration and Customs Enforcement, and the Internal Revenue Service Criminal Investigation Division) assigned to the investigative process of identity theft cases and cooperation is needed to successfully dispose of the crime.

Mandating that all financial institutions be required to report identity theft cases to law enforcement would be a huge step forward in overcoming this barrier to effective investigations. The Identity Theft Assistance Corporation is one agency that supports efforts to facilitate the exchange of information between the private sector (financial services industry, retail, health care, and telecommunications) and law enforcement agencies (Gonzales, 2007). All of these entities possess information that can be vital to the investigation and prosecution of identity theft crime, and cooperation is needed on the part of all those involved in a case to ensure a successful outcome. It is important for law enforcement to have access to commercial fraud information, which is usually much more extensive than the fraud information actually reported and submitted to local complaint databases.

Acquiring the cooperation from all those involved in a case of identity theft has proven successful in solving prior cases. One of the country's biggest identity fraud-heists ever

prosecuted in the United States involved the collaboration of computer security experts, the Department of Justice, the Secret Service, attorneys, and police departments from the United States, Turkey, Germany, Ukraine and Estonia (Pereira, et al., 2008). Without the continued cooperation of all these agencies, the identity thieves would have continued using stolen identities and more individuals and businesses would have fallen victim. Further, the Hillboro Police Department has implemented a program which allows suitably qualified individuals from the community to assist the police department with investigating internet related crimes providing expertise where police chronically lag behind criminals (Harrison, et.al, 2004). Evaluation of this program concluded that the program has produced positive results in solving crimes (Harrison, et al., 2004).

Police officers need to develop and move forwards with these types of programs with the intention of duplicating the success rates. This type of collaboration has also proved successful in the 2007-2008 GAO study in which GAO was able to track down individuals who were illegally selling and purchasing defense related items and refer proper cases to the police (GAO, 2008). It is clear that requiring information sharing and cooperation from various agencies has proven successful in the past to target criminals. Therefore, it is recommended that similar strategies be implanted in cases of identity theft.

Conclusion:

Undoubtedly, research is needed to determine where the downfalls lie in preventing identity theft crime and what can be done to alleviate the problem. The President's Identity Theft Task Force defines identity theft as "the misuse of another individual's personal information to commit fraud" (Roberson, 2008). Currently there is an inadequate system in place to track and investigate identity theft. Law enforcement officers agree that very few identity theft cases are

solved due to the anonymity of the crime, jurisdictional issues, and a lack of cooperation from many agencies (Owens, 2004). In an ordinary theft case, police can check for fingerprints and conduct interviews with witnesses but in cases of identity theft, the victim often has no idea how the perpetrator gained access to his or her information (Owens, 2004). Law enforcement faces multijurisdictional issues and inaccessibility of personal financial information during investigations. Measures need to be taken to strengthen the relationship between government, law enforcement, and the private sector.

The problem of identity theft has become more complex and challenging in recent years for consumers, businesses, and especially law enforcement personnel. Millions of victims have had to deal with the devastating losses accrued which have placed pressing demands on law enforcement implement effective strategies at combating the crime (Roberson, 2008). There are safeguards that can be put in place in the current system to overcome the challenges of investigating this crime. Reducing the opportunities for thieves to get access to personal information is critical in fighting this crime. Several recommendations have been made to stop identity theft from occurring and help track and prosecute identity thieves. It is evident that more resources are needed if law enforcement is expected to keep up with technology and the growing number of identity theft cases. Identity theft will never be stopped as long as personal information is available. However, successful initiatives can be allocated to alleviate the magnitude of the crime. It will take cooperation on the part of law enforcement, financial organizations, and consumers to have positive results.

Law enforcement officers are working to combat identity theft but face unique challenges that make their job difficult. The Task Force has recognized that everyone including consumers, the private sector, and federal, state, and local governments all have a role to play in fighting this

crime. There is no simple solution to combat identity theft as there are a growing number of problems associated with collaboration efforts and advanced technology. Public concerns about the security of personal information and identity theft remain high, and criminalizing identity theft has proven to not be enough of a deterrent for committing the act.

The Federal Trade Commission (FTC) has estimated that nearly 10 million Americans become victims of identity theft each year (FTC, 2006). Improving the effectiveness of criminal prosecutions, protecting customer information, and improving assistance for victims are among the top priorities of the government's strategic plan to combat identity theft (Gana, 2007). Not only do identity thieves steal other's identifying information, they also steal their time, money, and security. Safeguards need to be put in place to protect consumer's time, money, and security and help re-pay them for their losses. Law enforcement needs to be trained on how to investigate these technologically advanced crimes so perpetrators are held accountable for their actions.

Tens of thousands of identity theft complaints are made each year but few cases are solved due to the lack of information available to law enforcement, budgetary constraints and more pressing cases that need to be solved. Compared to visible street crime, identity theft crimes are also vastly underreported. This pattern needs to change since the underreporting of crime leads to more unsolved cases. According to the President's Identity Theft Task Force Strategic Plan, identity theft investigations require a staff of detectives, agents, and analysts with multiple skills sets (Roberson, 2008). The effective collaboration of many agencies is necessary due to the growing complexity of identity theft cases and the success that cooperation has had in solving various other crimes. Plausible recommendations have been made including creating a national database, giving law enforcement access to financial fraud in private corporations,

developing collaboration with foreign countries, executing prosecutions, amendments to federal statutes and guidelines, and further training for law enforcement. Carrying out these recommendations has the potential to improve the current, inefficient system that is in place for tracking and investigating identity theft.

SECTION V: REFERENCES

Automated Fingerprint Identification System. (2008). Automated fingerprint identification system. Online article retrieved July 3, 2009 from http://www.fbi.gov/hq/cjisd/iafis.htm.

Aftergood, S. (2008). National crime information center. *Federal Bureau of Investigation.* Online report retrieved February 26, 2009 from http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm.

Allison, S., Lersch, K., & Schuck, A. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33(1),* 19-29.

Beccaria, C. (1963). On crimes and punishment. Trans Henry Paolucci. Englewood Cliffs, New Jersey: Prentice Hall.

Britt, P. (2009). Identity thieves hit a new low. *Information Today, 26(2),* 19-24.

Brunet, J. (2002). Discouragement of crime through civil remedies: An application of a reformulated routine activities theory. Online article retrieved April 19, 2009 from http://wcr.sonoma.edu/v4n1/brunet.html.

Cameron, K. (2008). Identity parade. *The Economist, 386(1),* 14-15.

Choo, K., Gordon, J., Rebovich, D. (2007). Identity fraud trends and patterns: Building a data-based foundation for protective enforcement. *Center for Identity Management and Information Protection.* Online report retrieved February 20, 2009 from http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf.

Dadisho, E. (2005). Identity theft and the police response: The investigation. *Police Chief Magazine, 72(3),* 1-9.

Federal Deposit Insurance Corporation. (2004). Putting an end to account- hijacking identity theft. Online article retrieved June 2, 2009 from http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

Federal Trade Commission (FTC). (2003). Identity theft survey report. Online article retrieved May 31, 2009 from http://www.ftc.gov/os/2003/09/synovatereport.pdf.

Federal Trade Commission (FTC). (2006). Identity theft survey report. Online article retrieved June 21, 2009 from http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

Foster, K. (2008). ID leaks: A surprising source is your government at work? *Consumer Reports, 73(9),* 28-32.

Gana, T. (2007). President's identity theft task force releases strategic plan. *Mortgage Banking, 67(9),* 110.

Gonzales, A. (2007). Combating identity theft- A strategic plan. *The President's Identity Theft Task Force.* Online report retrieved March 22, 2009 from http://www.idtheft.gov/reports/StrategicPlan.pdf.

Government Accountability Office. (2002). Identify theft: Prevalence and cost appear to be growing. Online report retrieved May 31, 2009 from http://www.gao.gov/new.items/d02363.pdf.

Government Accountability Office. (2008). Undercover purchases on eBay and Craigslist reveal a market for sensitive and stolen U.S. military items. GAO-08-644T.

Harrison, W., Heuston, G., Mocas, S., Morrissey, M., & Richardson, J. (2004). High tech forensics: Serving as a police reserve specialist. *Communications of the ACM, 47(7),* 49-52.

Heller, I. (2007). How the internet has expanded the threat of financial identity theft and what congress can do to fix the problem. *Kansas Journal of Law and Public Policy, 17(1),* 84-108.

International Association of Chiefs of Police. (2005). Law enforcement priorities for public safety: Identifying critical technology needs. Online article retrieved June 21, 2009 from http://www.theiacp.org/LinkClick.aspx?fileticket=76jsKsxCEB0%3d&tabid=392.

Keel, T. (2008). Homicide investigations: Identifying Best Practices. *Law Enforcement Bulletin, 77(2),* 1-9.

Levitz, J., Pereira, J., & Singer-Vine, J. (2008). U.S. indicts 11 in global credit card scheme. *Wall Street Journal, 1(11),* 1-5.

Lifelock. (2006). Lifelock: #1 in identity theft prevention. Online article retrieved June 23, 2009 from http://www.lifelock.com/?oplisting=0.

Majoras, D. (2006). Federal identity theft task force report. *FTC.* Online article retrieved April 1, 2009 from www.usdoj.gov/ittf/docs/issues_summary.pdf.

McNally, M., & Newman, G. (2007). Identity theft-A research review. *National Institute of Justice*. Online report retrieved February 24, 2009 from http://www.ojp.usdoj.gov/nij/publications/id-theft/welcome.htm.

McQueen, M. (2009). The menace in the machines---Cyber scams on the uptick in downtown. *Wall Street Journal.* NewYork: pg. D1.

Moore, S. (2009). F.B.I. and states vastly expanding databases of DNA. *New York Times, 1(21),* 32-62.

National Insurance Crime Bureau. (2000). National insurance fraud forum. Online report retrieved June 2, 2009 from http://www.insurancefraud.org/downloads/White_paper.pdf.

Nishi, D. (2007). Protect the digital frontier. *Career World, 36(2),* 12-15.

Owen, M. (2004). Policing privacy: Michigan law enforcement officers on the challenges of tackling identity theft. *Public Interest Research Group in Michigan, 1(1),* 1-18.

Roberson, C. (2008). Identity theft investigations. New York: Kaplan Publishing.

Sovern, J. (2009). New Javelin report finds 22% increase in identity theft victims. Online article retrieved April 1, 2009 from www. javelinstrategy.com.

United States Department of Justice. (2006). Fact sheet: The work of the President's identity theft task force. Online report retrieved March 23, 2009 from www.usdoj.gov.

Wagner, D. (2007). A comprehensive approach to security. *MIT Sloan Management Review, 48(4),* 1-2.