IDENTITY THEFT RISK ASSESSMENT OF MIDDLE TENNESSEE

By

CRAIG R. MOORE

A thesis submitted in Partial Fulfillment of the Requirements

for the Degree of Masters of Criminal Justice Administration

Middle Tennessee State University

May 2014

Thesis Committee:

Dr. Dennis Powell

Dr. Lee Wade

Dr. Deborah Burris-Kitchens

TABLE OF CONTENTS

LIST OF TABLES

Page

ABSTRACT

The FBI states that identity theft has been the fastest growing crime for more than five years and many experts believe this will continue to increase. There are countless ways an individual's personal information can be compromised, which creates a much higher likelihood of becoming a victim. Most experts agree one of the best ways to reduce the chances of victimization is to become educated about the risks and take precautionary measures. This study employed a simple survey mailed to a random sampling of middle Tennessee residents to assess their knowledge of identity theft. The purpose was to gauge respondent's knowledge of identity theft, associated risk factors and preventive measures.

Keywords: identity theft, risk assessment, white-collar crime, fraud, Tennessee

ACKNOWLEDGEMENTS

I chose this particular topic because I know about and have extensive experience dealing with identity theft. During November 2005 until January 2010 I worked as an investigator for Kroll Fraud Solutions, a private company which provides security and risk consultation. While at Kroll, I worked with and spoke to countless victims of identity theft, gained considerable knowledge about the crime and witnessed how these incidents negatively impact the lives of the victims and their families. Consequently, it became my desire to help consumers avoid the pitfalls of identity theft by increasing awareness concerning the crime and providing better education, such as some of the practices discussed herein, to help avoid risky behavior.

This research project would not have been possible without the encouragement and support of my wife and her determination for me to ultimately complete it. I would also like to express appreciation to the professors in the Department of Criminal Justice at Middle Tennessee State University. I am very grateful for the lessons taught by Dr. Dennis Powell and the guidance offered by Dr. Lee Wade. Finally, I could not be where I am today without the help of my father and mother and I truly appreciate their assistance and willingness to proofread and offer insight. There have been many changes since this project began, but the one constant has been the support of those around me and their willingness to help.

CHAPTER I: INTRODUCTION

According to the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC) identity theft is a complex and growing problem; for several years in a row, the FBI has named identity theft as the fastest growing crime in the United States (FTC, 2003). In 2006 it was estimated there were 8.3 million victims and by 2009 it was estimated that number grew to over 11 million (FTC 2006, 2009).

Identity theft is not only increasing at a steady pace, but can be especially harmful to individuals unaware they have been victimized until their credit is ruined. Victims may have trouble obtaining credit, utility services, government benefits, or even employment and some have been arrested for crimes committed by someone who stole their identity. In addition to being harmful and irritating, identity theft incidents also take time and resources to resolve.

Identity theft is not a new phenomenon, since history shows individuals and "deities" have been stealing identities since the beginning of civilization; Greek, Egyptian and Norse mythology all describe occasions when an individual or entity used the identity of another for gain (Leonard & McClure, 2004). The Biblical story of Jacob and Esau is another example of identity theft (Genesis 27, New International Version). In the Book of Genesis, Jacob steals Esau's identity to deceive their father and claim the family birthright. In this story Jacob changes his appearance and smell to mimic that of Esau to fool his father Isaac. Over time however, identity theft has made a transition from appearance centered trickery to information-centered fraud, and technology has aided in this transition. Today, individuals are usually identified by a number (i.e. Social Security number, bank account

number, employee ID number, etc.) which, coupled with new technology, has made identity theft more commonplace with thousands of new victims each year.

Technology has made life more convenient but has also increased an individual's vulnerability. Twenty or thirty years ago writing a check was necessary to pay expenses but with today's technological advances, a savvy individual can do so on a phone, tablet or computer. Many banks allow customers to photograph checks for digital deposits and it's possible to transfer large sums of money via the internet. Technology has made life more convenient but has also opened a new world of high-tech fraud.

This study focused primarily on identity theft because The Federal Trade Commission's fraud survey of 2012 reported that identity theft makes up 18% of all complaints submitted (FTC, 2012). Identity theft can be very harmful particularly when the public is not aware of the risks of becoming victimized. This study is a risk analysis and assesses the identity theft knowledge of the respondents to determine knowledge of the credit reporting system, since experts agree that periodically reviewing credit reports is an excellent way to discover and prevent identity theft (FTC, 2012). Determining the general public's knowledge of identity theft should aid in the development of fraud mitigation tools and techniques.

CHAPTER II: LITERATURE REVIEW

Do you know what to do if you receive a letter explaining that you owe thousands of dollars for purchases made at your favorite home improvement store? What if the IRS informs you that someone has already filed your taxes and stolen your refund? You might be a victim of identity theft. Identitytheft.org defines identity theft as "the taking of a victims identity to obtain credit, credit cards from banks or retailers, steal money from victims' existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file bankruptcy, or obtain employment using the victims name." Stated more simply, it is the process of using someone else's personal information for your own personal gain (SpendonLine.com, n.d.).

Identity theft did not become a popular crime until the 1990's (FTC, 2000); however, the term "identity thief" first appeared in a news article in 1966. The Athens Messenger, an Ohio newspaper, ran a story about a man who used an acquaintance's name and date of birth to enlist in the Marine Corps because he felt his criminal record would disqualify him from serving.

It is unclear when identity theft first occurred, but banks and creditors first started issuing credit cards in the 1950's (Starbuck-Gerson & Woolsey, 2009). During this time period, identity theft was very rare and laws did not exist to deal with identity thieves (Starbuck-Gerson & Woolsey, 2009). In order to get credit in the 1950's and 1960's one would have to personally appear before a bank representative and he would "vouch" for the individual's credit worthiness, so committing fraud was rare (Starbuck-Gerson & Woolsey, 2009). The term "instant credit" did not exist, so a thief would be forced to forge several forms of photo identification to commit fraud and it was not easy or commonplace.

In the 1970's, credit card fraud and other forms of identity theft began to increase (Starbuck-Gerson & Woolsey, 2009); however, the crime was still considered rare and not nearly as common as it is today. In 1974, Congress passed the Fair Credit Billing Act to establish rules for creditors and mandated that portions of the law address fraud (Biegelman, 2009). The FICO (Fair Isaacs Corporation) credit scoring system began in 1960 but did not become a common way to determine an individual's credit risk until the 1970's (Biegelman, 2009). This new scoring system and the new availability of credit, meant thieves could steal an identity by obtaining an individual's social security number and a few other pieces of personal information.

Although sporadic during the 1970's and 1980's, identity theft did not become popular until the 1990's with the dawn of the Internet (FTC, 2005). The Internet meant two things to criminals; potential easy access to large caches of data and anonymity. Many financial institutions began storing, transferring and communicating via the Internet which causes security to be problematic because technology makes it easy to obtain information via a variety of avenues (Poneman, 2009). Applying for credit via the Internet is commonplace and even with today's knowledge of fraud it is relatively easy for a person to request a credit card using someone else's information. In addition to credit card fraud, identity theft can affect a bank account or may be used to establish utility service. Identity theft can take many forms and each method uses slightly different means to accomplish its goal but all forms are crimes and some of the most common types are presented below.

Types of Identity Theft

Check fraud could result from a lost or stolen checkbook, and entails illegal access to someone's checking account. Technology has enabled criminals to create a phony

checking account based on stolen banking information which allows criminals to write checks before the fraud is recognized. Many retailers use check verification companies like Certegy or Crosscheck to validate check transactions and these companies can electronically stop a check purchase if fraud is suspected. Check fraud theft can range from hundreds to thousands of dollars, but once the account has been cancelled and the check verification company notified, the checks are no longer supported by legitimate funds. A victim of check fraud will not be held financially liable unless he is suspected of playing a role in the fraud or if the bank is not alerted within 60 days after it occurs. Banks and retailers usually absorb the loss whenever check fraud is committed.

Benefits fraud is committed in order to obtain some sort of government benefit; local, state or federal and entails the use of personal identifiers to obtain tax, welfare, unemployment or healthcare benefits. In order to commit this crime one must possess knowledge of the benefits system and all of the personal identifiers of another. This type of fraud is relatively rare because the benefits received are considered meager compared to other, more profitable, types of identity theft. Victims of benefits fraud must work with the applicable government agency to resolve the issue which can be a long and arduous process because of government inefficiencies. Taxpayers are usually responsible for the expense of benefits fraud and generating the lost revenue.

One of the most common types of identity theft involves opening a new credit card account. This can be done online, over the phone, or in person using someone else's social security number, address and mother's maiden name. Victim will not become aware of the problem until the credit card is over the limit or in default, which can adversely impact the victim's credit report. Credit card companies are familiar with this and they can resolve

the issue once it is identified; however, they are more likely to write-off the loss than attempt to prosecute those responsible. The lost revenue is absorbed by the affected credit card company and then passed on to the consumer via higher fees and interest rates. Credit issuers desire to make the application process quick and efficient, but doing so makes them vulnerable, as it is easy to obtain a fraudulent account. Credit card fraud accounts for 26% of the types of identity theft complaints submitted to the Federal Trade Commission (FTC, 2009).

Utility fraud consists of 18% of all identity theft related complaints reported to the FTC and is usually committed by someone unable to obtain or unwilling to pay for utilities (FTC, 2009). Common types of utility fraud involve gas, water, electricity, cable or phone service and occurs when a criminal supply's another individual's information. Utility service is provided based on the victim's credit rating and can continue until payments cease. It is common among illegal aliens and they will often steal or purchase a social security number in order to obtain the necessary utilities (Biegelman, 2009). Victims do not usually discover the crime until the fraudulent account has been turned over to a collection agency, which negatively affects their credit rating. Victims are not usually held financially liable for the fraud, but they must work to resolve any outstanding credit issues and submit proof to the affected utility company. Utility companies typically absorb the lost revenue and may raise their rates to account for the loss.

Medical identity theft has the potential to be life threatening, especially if urgent care is required, and it has two main aspects: 1) The perpetrator uses the medical insurance of the victim, leaving them to address any outstanding medical bills or 2) An individual supplies the personal identifiers of another at check in/patient registration. A problem arises when the

medical record associated with the perpetrator becomes associated with the victim, which can have dire consequences when drug allergies, blood types, past surgeries, etc. are taken into account. Another negative effect involves the denial of medical insurance and fraudulent medical bills. Furthermore, there is no central medical database like for credit related issues; so a victim would not necessarily become aware of any problems unless a medical bill is received. Each State obtains and maintains medical records in a different manner, so what may be true in one State may not be true in another. In February 2010, the Poneman Institute conducted a survey on medical identity theft and found that almost 1.5 million Americans have been victimized with an estimated cost of $28.6 billion dollars. The cost and potential life threatening consequences of medical identity theft make it a serious issue that consumers must be aware of.

Identity thieves may also access a bank account or use someone's information to create fraudulent bank accounts. This is a common complaint according to the Federal Trade Commission and makes up 17% of complaints. This type of identity theft is difficult to perpetrate because banks want several forms of ID, and a criminal must have these in hand and be able to answer questions concisely so as not to draw suspicion. Bank fraud can leave a mark on a victim's credit report and a victim may be harassed by debt collection agencies or a judge may issue an arrest warrant for issuing bad checks. Much like credit card fraud, banks usually absorb the monetary loss unless the perpetrator can be brought to justice and restitution garnered.

Employment fraud is popular among illegal aliens, because most employers require a social security number prior employment. Although employers are advised to verify the legitimacy of an applicant's social security number, it does not always happen; nor

is there a federal law requiring ID verification. In 1997, the Immigration and Naturalization Service (now Immigration and Customs Enforcement—a division within The Department of Homeland Security) and the Social Security Administration teamed up to create E-Verify, an easy to use Internet based system to compare Social Security records with employment applications (United State Citizenship and Immigration Service [USCIS]). The program has grown steadily and is used to prevent, among other things, employment fraud. A possible shortcoming of E-Verify is that it is a voluntary program and employers are not required to verify an applicant's social security number.

Employment fraud is different than other types of identity theft because the illegal use of one's social security number can affect the amount contributed to Social Security and the way one's taxes are calculated. The Internal Revenue Service (IRS) cannot differentiate between legitimate and illegitimate employment unless it is notified, and a victim could be held responsible for back taxes until he provides evidence to support an identity theft claim. For many victims, dealing with the IRS is a long process that involves numerous written exchanges, which may affect the delivery of tax rebates, tax refunds or other government benefits. According to the FTC, 12% of complaints involved employment fraud (FTC, 2009). The exact number of employment fraud victims is unknown, but each tax season is a reminder of the severity of the problem as more victims are identified.

Tax refund fraud is another IRS related scam which occurs when a criminal uses the social security number of another or a minor child to steal a tax refund or file a dependent claim. This is the third largest source of theft from the federal government and accounts for roughly $5 billion in losses (Starkman, 2013).

Criminal identity theft occurs when an individual poses as another during the commission of a crime, or while in violation of the law an individual provides false identifying information (driver's license, social security number, etc.) to law enforcement during an arrest, traffic stop, or investigation. This can profoundly impact the victim and result in an arrest until fingerprints or photos can be compared to that of the perpetrator. Criminal identity theft can take years to surface and leaves the victim to determine the jurisdiction where the incident occurred, how to resolve it, and pay for attorney fees. Victims may be ordered to appear before a judge even though there may be a great distance between the victim's residence and where the crime occurred. Victims are required to obtain photos and fingerprints to submit to the arresting agency for comparison and many states now advise victims to have an identity theft passport on them at all times. The identity theft passport is an official document that indicates criminal identity theft has occurred and extra steps should be taken to confirm the identity of the passport holder. The passport is issued by the state or a law enforcement agency and is especially important to have during routine traffic stops so as to avoid an unwarranted arrest. Criminal records associated with the identity theft can falsely be associated with an innocent person and can create a false stigma or result in employment hardships. Many businesses, leasing companies and government agencies conduct criminal background checks to determine employment suitability, evaluate risk and ensure that new hires do not have a criminal record. Criminal identity theft is a very serious crime and can profoundly impact the life of the victim.

Identity Theft Prosecution

Although punishment and prosecution rates vary, identity theft is a crime in all 50 States and it is recognized by Interpol as a growing international threat (Biegelman, 2009).

Each state varies but identity theft is considered either a felony or a misdemeanor depending on the severity of the crime and the amount of money, goods, or services stolen. Those convicted on the state level can expect to serve time in prison and most states impose fines of up to $100,000 and order the offender to provide financial restitution.

In 2004, Congress enacted the Identity Theft Penalty Enhancement Act, which increases punishment and sets predetermined prison sentences for those convicted of committing identity theft (Biegelman, 2009). The Identity Theft Penalty Enhancement Act also formally established the crime of "aggravated identity theft" and mandated a federal prison term for those convicted of the crime. The Identity Theft Penalty Enhancement Act established punishment standards for those convicted of identity theft in support of terrorism and increased the penalties for those individuals who possess access to personal and financial information on a large scale.

Impact of Technology

There are many ways someone's identity can be used fraudulently and some methods may be more harmful than others. Identity theft is a relatively new crime but as it grows consumers, law enforcement, lawmakers and businesses must consider the impact of technology and how technology plays a role in its growth and prevention.

One of the reasons identity theft has become commonplace is because of technology. In 2005, retail giant TJX (the largest off-price fashion and apparel retailer in the US) lost 45.6 million credit and debit card numbers as well as the personal data of about 451,000 individuals because someone was able to hack into the system that stored the information (Vijayan, 2007). The amount of information that is stored digitally or accessible

via the Internet is astounding. This technology improves business but it also creates a tempting target for criminals.

The amount of information that businesses and government agencies maintain is substantial and they must go to great lengths to safeguard it. Internet security has grown to a $58 billion dollar industry but there are still many ways an individual can fall prey to scammers (Walko, 2005). The internet has brought us closer to our friends and made shopping easier, but it has also brought fraud in to our living rooms.

The average American worker receives 13 spam messages a day which can contain viruses, spyware or other forms of malware (Nucleus Research, 2004). Malware is short for malicious software and it has the potential to damage a computer or may become intrusive. Conversely, the US Postal Service (USPS) has indicated that the average household receives 800 pieces of junk mail each year; none of which can be as detrimental as a single spam email that contains a virus, worm or malicious confidence scheme (USPS, 2007). Technology has increased our socialization, our consumption of goods and our risk of fraud and other identity crimes.

Twenty years ago, few people had access to account or billing information and a thief would have to break into a bank to obtain the information. Today, banking and personal information is floating through cyberspace or stored in places that may be accessible via the Internet. Information security is contingent upon the electronic safeguards, firewalls and data protection plan of a given business, individual computer or employee and occasionally each experiences a security breach. When a business or government agency loses a large cache of information it is called a data breach and it can negatively affect all parties involved, including those individuals who had their information compromised.

In 2010, the Ponemon Institute conducted a study and found that the average cost of a data breach was $7.2 million, or about $214 per compromised record. In January 2012, a private company called Advanced Occupation Medicine Specialists accidentally compromised the personal records of 7,226 patients (Privacy Rights, n.d.). A breach like this can severely damage the business's reputation and it can become very expensive or lead to closure. Each of the 7,226 individuals involved are at an increased risk of identity theft and the company is liable. Although laws vary by state, a company that has compromised client data may be held liable via fines, sanctions or through the litigation process.

The federal government is not immune to a data breach and it has experienced several losses. In 2006, the Veterans Administration (VA) admitted that an employee lost a laptop and data storage device containing the personal information (name, date of birth, social security number) of 26.5 million current and former servicemen and women. As a result of the data breach, a court ordered the VA to pay $20 million in damages (Yen, 2009). Government agencies and businesses must do everything possible to limit their exposure and they must take steps to limit their liability by safeguarding the information they possess.

Businesses and government agencies must also take precautions to limit their susceptibility to being hacked. A hack occurs when an individual or group of individuals electronically breach a business or entity with the goal of pilfering electronic data (personal information, account numbers or trade secrets) or transferring assets. Computer hacking is difficult for law enforcement to track as most hackers are able to maintain anonymity in cyberspace. In 2009, hacker Albert Gonzalez electronically stole roughly 130 million credit and debit card numbers by hacking into several large retailers (Poulsen, 2010). Gonzalez was later caught and sentenced to a new record in regards to identity theft sentences, 20 years

(Poulsen, 2010). The Privacy Rights Clearing House is a non-profit data watchdog and they estimate that more than 500 million records have been compromised since 2005.

Consumers must take steps to reduce their risk and protect their personal information and the identity theft protection, mitigation, notification and resolution industry has grown ten fold (Greenberg, 2010). Companies like LifeLock, Identity Guard, Debix, ID Watchdog and Identity Theft Shield have become popular and offer various versions of an identity theft service that help victims resolve identity theft related problems or monitor an individual's credit reports. Each of the three consumer credit repositories (Equifax, Experian & Trans-Union) now offer some type of identity theft service and most insurance companies offer an identity theft protection or recovery plan. Although an exact number is elusive, it is estimated that the identity theft protection/resolution industry has grown to over a billion-dollar industry which is remarkable considering the industry did not exist until about 10 years ago (Greenberg, 2010).

Technology has opened the door for hundreds of new scams and other malicious intentions where websites like Myspace, Facebook, Craigslist and Twitter are being used to obtain personal information and perpetrate fraud. Likewise, social media websites have been used to perpetrate confidence scams, burglary and identity theft. Consumers must be aware of the risks and leverage technology to protect their information by regularly reviewing credit reports and financial statements and shredding important documents. According to a 2010 Javelin Research study, the consumer identity theft protection industry has grown into a $2.4 billion market and in 2008, nearly half of all American adults paid for some sort of identity theft protection service (Javelin, 2008). In 2006, the FTC estimated that identity theft cost

roughly $45 billion despite the vast sums of money spent trying to prevent it and the unauthorized release of consumer information.

Technology is to fraud as protection is to cost and each shares an uneasy relationship. Companies like Norton, McAfee, and AVG make millions of dollars working to preemptively stop and neutralize all current and evolving Internet threats and scams. The cost of fraud is substantial and the Internet Crime Complaint Center or IC3 (a partnership between the FBI and the National White Collar Crime Center to research and investigate various crimes) estimates that in 2009 Americans lost more than $550 million in Internet fraud and scams (IC3, 2010). Fraud is an evolving threat that encompasses many types of scams and illegitimate transactions. It affects millions of people each year and costs the global economy roughly $500 billion annually (Baxter, 2009). In sum, fraud is a very expensive, wide-ranging problem that is positively impacted by society's new and evolving technologies.

Current Events

Between 2006 and 2007 many large banks, creditors and mortgage companies began adjusting their business model and downgrading their profit outlook as an economic downturn began to surface. Nearly a year after the problems surfaced, the great economies of the world began to suffer and as a result of the financial crisis, the International Monetary Fund estimates that global bank losses were roughly $2.28 trillion (Crutsinger, 2010). The Wall Street Journal called the situation the worst financial crisis since the Great Depression (Hilsenrath & Paletta, 2008). Though it's difficult to pinpoint the exact cause, the financial crisis was a result of excessive debt and inflation which caused several large mortgage companies to declare bankruptcy. The U.S. Government provided several "bailouts" to

various key businesses and unemployment, national deficits, mortgage defaults and foreclosures increased. The financial growth of first world countries stopped and blame for the crisis was placed on over-zealous consumers, greedy corporations, and the federal government with its regulation of the lending industry. The current financial downturn sets the stage for an extended and difficult job market and potential increases in fraud and identity theft.

In January 2009, risk consulting firm Kroll released their quarterly fraud report which discusses how fraud will increase as the global economy suffers. The report warns businesses about fraud in the context of the changing economy and explains that as the economy worsens, businesses must compete more feverishly for the available income. Likewise, lackluster employment options mean individuals may look for income sources that are not legal.

In a poor economy businesses must do everything possible to limit their risk, which includes reducing their liability when it comes to employees. Many businesses reduce their risk by conducting background checks on potential employees. One example of this type of liability occurred when a Countrywide Mortgage employee was arrested for pilfering the personal information of two million Countrywide loan applicants (Reckard & Menn, 2008). Many employers now require background checks that include a review of an applicant's credit report.

In today's economic climate, both consumers and businesses must be aware of the risks and impact of identity theft and other forms of white collar fraud. It is important that businesses and consumers reduce their risk by being knowledgeable and by regularly reviewing credit reports. Legitimate employment options are limited and very competitive so

job seekers must take every opportunity to highlight their talents and present themselves as honest individuals. Likewise, businesses cannot afford to hire individuals who possess a criminal record or have the potential to defraud the company. This is especially important for those just graduating from college and entering the job market for the first time as it is especially difficult if an individual's credit report reflects a potential liability.

Identity Theft Demographics

In 2006, about 8.9 million people claimed to be victims of identity theft while financial losses during 2006 were roughly $56.6 billion dollars (Javelin, 2008). Javelin Research determined that on average each victimized consumer was defrauded for about $6,278 and spent about 40 hours trying to repair the damage caused by identity theft.

Identity theft has several aspects and to get to the root of the problem one must ask and answer several questions: 1) how does identity theft occur, 2) who is victimized by and who commits identity theft and 3) where are people most likely to be victimized?

There are several ways identity theft can occur but recent statistics reveal the largest percentage of victims have either lost or had their personal information stolen (U.S. DoJ Bureau of Justice Statistics, 2010). SpendonLife.com reports that low tech methods like stolen wallets and documents account for 43% of all identity theft incidents while online victimization only occurred 11% of the time. Some common avenues for identity theft include a deceitful friend or relative, a dishonest employee or via stolen mail. Dumpster diving is a term to describe the lengths an identity thief will go through to obtain personal or financial data and there have been reports of businesses, schools and government offices carelessly discarding sensitive information by throwing it in an easily accessible trash receptacle.

The question of "who" has two aspects--the victims and the perpetrators. The tech-savvy 18-24 demographic is most often victimized and the 2005 Bureau of Justice Statistics report (NCVS) on identity theft indicates that the 18-24 demographic is twice as likely to be victimized as seniors aged 65 or older. The 25-64 age group, although numerically superior, is only slightly less often victimized. It is theorized that the 18-24 demographic are victimized because they may not be as cautious with their personal information and may be ignorant of the crime and the credit reporting system. Identity thieves are aware of this and can use a young adult's "blank" credit history to begin establishing lines of credit. In a study conducted by the Chubb Group, it was learned that 30% of college students that were surveyed discard credit card applications without shredding them and ignore their checking and credit card statements. These relatively minor mistakes do not entirely explain the high victimization rates among 18-24 year olds but they do warrant a closer investigation and they indicate a level of carelessness.

A 2003 Federal Trade Commission study reveals 76% of identity theft perpetrators are unknown, while the remaining 24% of victims know the identity of the perpetrator through a financial institution or a personal relationship. Recent Department of Justice statistics reveal most individuals who are arrested for identity theft are also charged with additional crimes (i.e., property crimes, drugs, fraud, etc) and there are a broad range of individuals who are typically associated with the crime (methamphetamine dealers and users, organized crime syndicates from the Balkans, and illegal aliens).

New account fraud can be committed by a variety of individuals but an FBI/NDIC (National Drug Intelligence Center) bulletin indicates individuals who manufacture and/or use methamphetamines are likely to be responsible. Benefits fraud involves obtaining

government benefits by using someone else's information and is often committed by illegal immigrants. Immigration or illegal immigration is synonymous with identity theft and most employment, utility and some tax fraud is blamed on illegal immigrants (Biegelman, 2009). The immigration issue also explains where identity theft occurs.

According to a 2009 study by the FTC, Florida has the most identity theft related complaints, while California, Arizona, Nevada and Texas round out the top five states with high incidence of identity theft. It should be noted that each of these states has a large immigrant and illegal immigrant population and each is considered a border state. This is noteworthy as lawmakers, law enforcement officials, and financial institutions need to learn to effectively address identity theft in these states.

Identity Theft Resolution

Identity theft affects millions and costs billions and the crime has been increasing for several years in a row. The crime burdens society and each person who is victimized. Those affected generally resolve their problems without the aid of law enforcement because most agencies are hesitant to get involved as identity theft is rarely prosecuted because it is difficult to locate those responsible. Furthermore, the crime is often viewed as a victimless crime because many financial institutions absorb the monetary loss and may not seek prosecution unless the dollar amount is excessive.

Although the laws dealing with identity theft have been strengthened, those arrested for the crime are more easily prosecuted for associated ancillary crimes like drug possession or theft. Due to the widespread nature of identity theft, inconsistent definitions and varying jurisdictional prosecution issues, prosecution rates are difficult to measure. One of the recommendations made by a 2012 Congressional Research Service report was to

increase the prosecution and punishment of identity thieves, even though those found guilty of committing the crime have received harsher punishment since 1998. At least one identity theft ring was able to continue its "trade" while incarcerated in federal custody (Siciliano, 2011). Regardless, the number of identity theft complaints far outweighs the number of individuals who are federally or locally prosecuted (Congressional Research Service, 2012). The burden of proof usually falls on the consumer and many financial institutions do not have the resources to investigate every incident. Consumers can have a very difficult time documenting their true identity and the crime is burdensome because few know how to resolve it or the applicable laws that address it and the credit reporting system. Most victims do not know the correct course of action following an incident or that the average amount of time to resolve it can range from 20 to 40 hours and cost about $400 dollars (Javelin, 2009). Consumers quickly learn that the crime is frequent, difficult to detect, expensive, and difficult to resolve, which is why these factors make identity theft a real and confounding issue for consumers and victims.

Experts agree that the victimized should immediately place fraud alerts and request a copy of their credit reports (FTC, 2009). This is easy to do and can be done by making a phone call or visiting the website of one of the three major credit repositories. Fraud alerts add a specific statement to a credit report and advises creditors to take extra steps to verify the validity of any new credit applications. The three credit repositories also offer a credit freeze, which restricts all access to a credit file so obtaining new credit/financing is nearly impossible.

Ordering and reviewing credit reports will give the consumer an overview of the damage done by the imposter; however, some types of identity theft do not involve the credit

system and will require different resolution procedures. Once a credit report is obtained, it is necessary to file a police report to add credibility, show willingness to prosecute and to demonstrate being a victim. The victim must contact each creditor, retailer, or affected business and specifically explain the situation and provide the police report and documentation to prove the validity of their identity (i.e., signature cards, fingerprints, driver's license, social security card, proof of address, photos, etc.). It will also be necessary to contact each credit reporting agency and dispute any erroneous information. The credit repositories and affected businesses will conduct an internal investigation and provide notice of the results. Most businesses are able to recognize identity theft and absolve the victim of any financial responsibility; however, this can take anywhere from one to six months. Occasionally, a business will not recognize the fraud and the victim must take additional actions such as contacting a government regulatory board or a state attorney general. Criminal identity theft, check fraud, medical identity theft and tax/benefits fraud have very similar resolution procedures and require victims to obtain a police report and provide proof of identity to each affected institution. Regardless of the type of fraud, victims must work on their own behalf and use their resources to fix what was perpetrated by someone else.

Identity Theft Prevention

Those who wish to prevent identity theft should protect their personal information by restricting its dissemination and by shredding documents that contain personal or financial data. Periodically reviewing credit reports and monitoring bank, credit, tax, social security, and utility statements are also good practices. However, it is important to remember that there are numerous private and government institutions that possess one's personal

information and these institutions are only as secure as their data protection plan and the integrity of their employees.

Individuals must be aware of identity theft as many are vulnerable simply because they are unaware of the crime or know how the credit system functions. Unlike some crimes, identity theft does not discriminate based on race, age, or socioeconomic status as it has been known to affect celebrities, small business owners, government officials, CEOs and blue-collar workers. An identity theft issue can have the potential to leaving a long-lasting mark on an individual's history and can cost thousands of dollars.

American consumers are victimized by identity theft at an alarming rate and experts agree that knowledge of the crime is one of the best ways to prevent it. Suffering an identity theft incident can be especially unnerving because a criminal is fraudulently using someone else's identity – a very personal concern. This study is a risk analysis of the middle Tennessee area and it assesses the identity theft knowledge of the respondents.

CHAPTER III: METHODS

The goal of this research project is to determine if efforts to educate the public concerning identity theft have been successful. This study should also determine if identity theft education is still lacking or if those efforts are reaching a broad sample of the public. This project studied a relatively small, random sample of individuals in the middle Tennessee area and conclusions about the general population should not be garnered based on the results.

This project sought to answer three questions: 1) Does education correlate with "knowledge" of identity theft, 2) Does race/gender correlate with "knowledge" of identity theft, and 3) Are respondents familiar with identity theft best practices but not the credit reporting system or vice versa? It was hoped that each of these questions would be answered at the study's conclusion. The first two questions ask whether demographics and education play a role in an individual's awareness or knowledge of identity theft crime, while the third question tries to determine if individuals are familiar with the credit reporting system but not the many ways to reduce the risk of identity theft or vice versa.

Reviewing one's credit report is a good way to determine if identity theft has occurred and it is feared that many may not be aware of the significance of periodically reviewing a credit report. The aforementioned research questions are straightforward and should indicate how to better or who to better educate regarding identity theft.

Due to the high incidence of identity theft, the government, various consumer watchdog groups and businesses now provide information about it, avoidance, and ways to cope should it occur. Identity theft has continued to increase despite educational efforts, so it remains to be seen if consumer knowledge has been a factor in reducing the incidence of the

crime. By using a random sample of individuals from middle Tennessee this research project was able to ascertain general identity theft knowledge and the information can reasonably be applied to larger samples in Tennessee or the greater southeastern United States; however, further research is necessary due to the small sample size.

Survey Instrument

The survey was designed to be a simple and effective way to determine a respondent's knowledge of identity theft and the credit reporting system. It was initially hoped that respondents would not be put off by the length or complexity of the survey and thus provide a favorable rate of return. The survey consisted of simple Yes/No questions and it contained no complex terms or phrases that an average person would not understand. The questionnaire was titled "Identity Theft Knowledge Survey" and was administered with a statement indicating participation was voluntary and all information would be kept confidential. The survey was targeted at those 18 years of age or older and consisted of 14 questions related to identity theft and the credit reporting system as well as five demographic questions and one multiple-choice question.

Each question was designed to be easily understood and there were no industry-specific or confusing terms. The format was similar and those questions with similar subject matter were grouped together. Each question asked respondents about their personal experiences and behaviors and to answer each question honestly by circling their responses. The questionnaire was intentionally made very simple and easy to complete so as to increase the rate of return and to be able to reach the broadest spectrum of potential respondents. It was also kept uncomplicated so as to simplify the data analysis and eliminate coding confusion.

The final question asked respondents about the age group that is most often victimized by identity theft and is the only question that required any prior knowledge. It was included in an effort to gage consumer awareness with regard to future research and it was intended to expose a possible stereotype.

Sample

Respondents were randomly selected from a Williamson County phone book and surveys were mailed to 400 individuals in the Tennessee cities of Franklin, Brentwood, Arrington, College Grove, Thompsons Station, Nolensville and Fairview. Those selected to receive a questionnaire also received a brief letter advising them of the purpose of the survey and a pre-addressed, pre-stamped envelope to make the return process free, easy, and convenient.

Williamson County is located in middle Tennessee and is roughly 584 square miles. The county is located directly south of Nashville; Tennessee's capitol city. The population of Williamson County is estimated to be 183,180 and the racial distribution is as follows; 89.5% white, 4.7% black, 3.9% Hispanic, and 2% Asian. The largest age group are those 45-54 with 16.4% of the population; the second largest group are those 55-64, followed by 25-34 and 35-44 at 12.9% each, those aged 20-24 and 65-74 make up 6.5% each, those older than 75 make up 3.8% and the remaining percentage of population (27.6%) are considered minors and were not included in this survey. Most households in Williamson County earn more than $50,000 annually and a majority of Williamson County residents have had at least some college (US Census Bureau, 2010).

According to a 2010 study by the Federal Trade Commission, Tennessee ranks 24th in reported incidents of identity theft compared to other states. Only the metropolitan

area of Memphis is ranked among cities with considerable identity theft complaints in the state. In the same study, the FTC reported benefits/government fraud as the most common type of identity theft related complaint in Tennessee, followed closely by credit card fraud. Williamson County was chosen as a convenience sample because of its proximity to Middle Tennessee State University and the author's residence. It also proved to be a good area of study due to the relative affluence and degree of education of its residents. Williamson County publishes its resident's full address in the county issued phone book so obtaining a random sample of the population was free and convenient.

Procedure

In order to properly understand the data collected, the researcher employed descriptive statistics which provide summaries about the sample and the variables as well as a quantitative analysis. Descriptive statistics are useful for simplifying data but cannot be used to collect any type of explanation beyond what the data suggests. For example, descriptive statistics can summarize the attitudes of middle Tennessee residents regarding identity theft but they cannot explain why middle Tennessee residents retain those attitudes--they are a quantitative tool as opposed to a qualitative analysis. The author utilized Pearson's R and Statistical Package for the Social Services (SPSS) to break down the data and present it in a manner that could be understood and interpreted.

Karl Pearson was a statistician and scientist in the early 20th century and he created a formula that could be used to analyze data (Rumsey, 2011). Pearson's formula provides a value between +1 and -1 where +1 is a perfect or very strong correlation, -1 is imperfect and 0 has no correlation. It is used to measure the strength, or correlation, between two variables. Pearson's R was used to measure the correlation between the demographic

data, the survey questions and the answers each respondent provided. The values for each correlation are provided in the following chapter.

Although Pearson's R is used commonly and does an adequate job of analyzing large data sets, there is one main weakness that needs to be mentioned (Rumsey, 2011). The correlation that is highlighted by Pearson's formula does not necessarily display causality, so it may be difficult for a researcher to determine the responsible parties in regards to each variable. This is particularly evident when the relationship between the variables is non-linear. These weaknesses force the researcher to make certain assumptions that are not necessarily based on fact and may influence the interpretation of the data.

Upon receipt of the completed surveys, each questionnaire was numbered and each question and answer was given a value with a designated number. The variables in this study are the respondent's answer to each question and each variable was also assigned a value. The coded surveys and each variable were then entered into a statistical computer program called SPSS.

Statistical Package for the Social Services and later called Statistical Product and Service Solutions (SPSS) was created in 1968 by Norman Nie, Dale Bent and Hadlai Hull and is commonly used in the social sciences to determine frequencies, summarize data, determine variances and variables and can be used to create graphs or charts (Field, 2009). SPSS is similar to many commonly used computer programs (i.e. Microsoft Excel, etc.) and is intuitive and user friendly. Once the data has been entered, an SPSS user only needs to instruct the program how to display the resultant information. SPSS has few disadvantages because its success or failure depends solely on the individual coding and entering the data (Field, 2009). For the purposes of this research project, the data was broken down between

each survey question and the demographic data that was requested from each respondent. The resulting SPSS graphs are provided in the following chapter.

CHAPTER IV: RESULTS

Of the 400 questionnaires mailed to random individuals in the middle Tennessee area, 134 individuals completed and returned the surveys – a return rate of about 34%. This does not account for any surveys that may have been misplaced by the US Postal Service either going to potential respondents or those returned from respondents. Also, because of discrepancies on returned surveys (incomplete, multiple answer selections, etc.) some were discarded or unusable. For the purposes of this research project, 125 completed surveys were included in the statistical analysis. As mentioned in the previous chapter, SPSS was used to code and analyze the data and provide the following descriptive statistics.

The questionnaire asked each respondent to provide his or her demographic information and to select their sex, appropriate age group, ethnicity, education, and area of employment from a list of options. Of those that responded 54% were male and 46% were female.

Table 1

Demographics: Gender Distribution

Gender	Frequency	Percent	Valid Percent
Male	67	53.6	53.6
Female	58	46.4	46.4
Total	125	100.0	100.0

The most common age group represented was the “40-50” group garnering 28% of the responses; the next most represented age group were those “51-61”. The lowest age group represented were those “84-94”, with only about 2% completing and returning the surveys.

Table 2

Demographics: Age Distribution

Age Group	Frequency	Percent	Valid Percent
18-28	4	3.2	3.2
29-39	22	17.6	17.6
40-50	35	28.0	28.0
51-61	28	22.4	22.4
62-72	27	21.6	21.6
73-83	7	5.6	5.6
84-94	2	1.6	1.6
Total	125	100.0	100.0

The ethnicity question was the least diverse with 90% of the respondents calling themselves “White (non-Hispanic)”. The next highest group were those who label themselves “other”, but it was only 3% of respondents. These statistics coincides with US Census data.

Table 3

Demographics: Ethnicity Distribution

Ethnicity	Frequency	Percent	Valid Percent
Asian	3	2.4	2.4
Black	2	1.6	1.6
Hispanic	3	2.4	2.4
White	113	90.4	90.4
Other	4	3.2	3.2
Total	125	100.0	100.0

The level of education question asked each respondent to select his/her highest level of education and ranged from "High School/GED" to "Post Graduate Degree". The highest represented group were those who hold a bachelor's degree (36%) while those who had no education or who selected "none of the above" were only about 1%. Those whose education stopped at high school were the same as those who indicated they have a master's degree (both 22%).

Table 4

Demographics: Education Distribution

Education	Frequency	Percent	Valid Percent
High School/GED	27	21.6	21.6
Associates Degree	7	5.6	5.6
Bachelors Degree	45	36.0	36.0
Masters Degree	27	21.6	21.6
Post Graduate Degree	18	14.4	14.4
None	1	.8	.8
Total	125	100.0	100.0

The final demographic question asked each respondent to provide his/her field of employment. The most common choice selected was the "professional" field of employment with 41%. The second most common response was "retired" with 23% indicating they are no longer gainfully employed. The "law enforcement" field was the least represented with only 1% indicating they have a career in that field.

Table 5

Demographics: Employment Distribution

Employment	Frequency	Percent	Valid Percent
Clerical	8	6.4	6.4
Construction	3	2.4	2.4
Professional	51	40.8	40.8
Law Enforcement	1	.8	.8
Sales	10	8.0	8.0
Service Industry	6	4.8	4.8
Retired	29	23.2	23.2
Other	17	13.6	13.9
Total	125	100.0	100.0

As stated previously, it was the author's intention to make a very simple, easily understood questionnaire that contained no confusing or industry specific terms. With the exception of the last question, each respondent only had two response options, "yes" or "no". The questionnaire included 14 questions that would indicate the respondent's general knowledge of identity theft and identity theft best practices.

The first question was "Do you know what identity theft is?" and was used as a baseline to determine if respondents were even familiar with the crime. The overwhelming response was "yes" with 99% answering in the affirmative.

Table 6

Do you know what identity theft is?

Response	Frequency	Percent	Valid Percent
Yes	124	99.2	99.2
No	1	.8	.8
Total	125	100.0	100.0

The second question asked each respondent if they knew how to respond to an identity theft incident, "Do you know what to do if you are a victim of identity theft?" The FTC and the three major credit bureaus recommend placing a fraud alert and reviewing credit reports but it is not certain if that message has been related to all consumers. Of those that responded, 73% are at least somewhat familiar with how to respond to an identity theft incident; however, due to the simplistic nature of the survey it is difficult to determine if the consumers that answered in the affirmative are truly familiar with the appropriate steps to take to mitigate an identity theft incident.

Table 7

Do you know what to do if you are a victim of identity theft?

Response	Frequency	Percent	Valid Percent
Yes	91	72.8	72.8
No	34	27.2	27.2
Total	125	100.0	100.0

The third question asked "Do you know someone who has been a victim of identity theft?" Because identity theft is a common crime with a large number of complaints reported to the FTC each year, it is not surprising that 55% indicated they know someone who has been a victim.

Table 8

Do you know someone who has been a victim of identity theft?

Response	Frequency	Percent	Valid Percent
Yes	69	55.2	55.2
No	56	44.8	44.8
Total	125	100.0	100.0

The fourth question is of a personal nature and asked "Have you been a victim of identity theft?" Considering the responses to the previous question and the high incidence of identity theft, it was surprising that only 22% of respondents indicated they had been victimized at one time by identity theft. Its possible that some have been victimized but remain ignorant of the fact.

Table 9

Have you been a victim of identity theft?

Response	Frequency	Percent	Valid Percent
Yes	27	21.6	21.6
No	98	78.4	78.4
Total	125	100.0	100.0

The fifth question is related to identity theft best practices and asked "Do you know what fraud alerts are?" Recall that fraud alerts put a statement on one's credit file that asks a credit issuer to verify the identity of the applicant before issuing credit. Seventy four percent of respondents indicated they know what fraud alerts are.

Table 10

Do you know what fraud alerts are?

Response	Frequency	Percent	Valid Percent
Yes	92	73.6	73.6
No	33	26.4	26.4
Total	125	100.0	100.0

Question six asked "Do you know there are different types of identity theft?" and alluded to the fact there are several types of identity theft (credit fraud, tax related identity

theft, benefits fraud, etc.). Of those that responded, 64% are aware that there are at least two types of identity theft.

Table 11

Do you know there are different types of identity theft?

Response	Frequency	Percent	Valid Percent
Yes	80	64.0	64.0
No	45	36.0	36.0
Total	125	100.0	100.0

Question seven is related to question six and asked "Do you know that identity theft can affect more than your credit report?" Often an identity theft incident that is not related to credit fraud may not appear on a credit report so it is important for consumers to be vigilant in other areas should criminal, tax, utility, or benefits fraud occur. Ninety percent of those that responded are aware of the fact that identity theft can affect more than just a credit report.

Table 12

Do you know that identity theft can affect more than your credit report?

Response	Frequency	Percent	Valid Percent
Yes	113	90.4	90.4
No	12	9.6	9.6
Total	125	100.0	100.0

Question eight begins a section of questions that are more personalized and asks "Have you ever reviewed your credit report?" Periodically reviewing ones credit report is an excellent thing to do to make sure no errors exist and also to determine if identity theft is present. Experts suggest reviewing a credit report every four months or at least twice a year

and this is especially important if undertaking a refinance or making a large credit purchase. Eighty eight percent of respondents answered in the affirmative and indicated they had reviewed their credit report at least once.

Table 13

Have you ever reviewed your credit report?

Response	Frequency	Percent	Valid Percent
Yes	110	88.0	88.0
No	15	12.0	12.0
Total	125	100.0	100.0

Question nine asked "Have you reviewed your credit report in the last six months?" and is related to question eight but is more specific. For identity theft purposes this question is more appropriate considering it is important to review a credit report periodically. Only 43% indicated they had reviewed their credit report in the last six months.

Table 14

Have you reviewed your credit report in the last six months?

Response	Frequency	Percent	Valid Percent
Yes	54	43.2	43.2
No	71	56.8	56.8
Total	125	100.0	100.0

Question ten continues on the trend of best practices but moves outside the area of credit reports and asks "Do you regularly review your bank, credit card and utility statements?" It is important to review all financial statements in order to make sure they are error free and to determine if anything suspicious has happened with an account. Nearly all,

97%, of the respondents indicated they regularly review their bank, credit card and utility statements.

Table 15

Do you regularly review your bank, credit card and utility statements?

Response	Frequency	Percent	Valid Percent
Yes	117	93.6	93.6
No	8	6.4	6.4
Total	125	100.0	100.0

Question eleven asked "Do you shred documents that contain your personal or financial information?" This question is related to a common identity thief activity -- dumpster diving. It is not uncommon for individuals and businesses to discard documents that contain personal or financial information and an identity thief only needs a few pieces of information to perpetrate fraud. Experts agree that shredding is one of the best ways to prevent someone from accessing your personal identifying information via the trash. For question eleven, 72% of respondents indicated they do shred important documents before discarding them.

Table 16

Do you shred documents that contain your personal or financial information?

Response	Frequency	Percent	Valid Percent
Yes	90	72.0	72.0
No	34	27.2	27.2
Other/Error	1	.8	.8
Total	125	100.0	100.0

Question twelve rounded out the best practices section and asked, "Do you take steps to reduce the likelihood of identity theft?" This question summarized the previous four questions and asked the respondents to rate their behavior when it comes to identity theft best practices. About 87% answered in the affirmative and believe they take appropriate steps. At least some respondents are aware that they do not take identity theft best practices seriously, while another possible explanation is that the respondents who answered "no" do not know how to reduce the likelihood of identity theft.

Table 17

Do you take steps to reduce the likelihood of identity theft?

Response	Frequency	Percent	Valid Percent
Yes	109	87.2	87.2
No	16	12.8	12.8
Total	125	100.0	100.0

Question thirteen asked "Can information on credit reports be used for employment hiring purposes?" This was included in order to gauge whether or not respondents knew of the importance of accurate information being reported on a credit report. Many employers will review a credit report as part of applicant screening and it is very important that consumers are aware of this fact. Seventy eight percent of respondents answered "yes" to question thirteen.

Table 18

Can information on credit reports be used for employment hiring purposes?

Response	Frequency	Percent	Valid Percent
Yes	97	77.6	77.6
No	23	18.4	18.4
Other/Error	5	4.0	4.0
Total	125	100.0	100.0

The final question was multiple-choice and asked the respondents to "Select the age group that you think is most often victimized by identity theft" and provided the responses of 18-34, 35-50, 51-65 and over 65. This question was included to determine if there were any stereotypes among the respondents as the FTC indicates the age group with the highest percentage of complaints are those 18-24 years old. Respondents answered this question by indicating the 35-50 age group is most often victimized (38%) followed closely by the over 65 age group (32%). The 51-65 and 18-34 age groups received 14% and 13% of the votes respectively. Although there are several possible explanations there was no way for respondents to knowingly answer this question correctly unless they have had prior identity theft statistics education.

Table 19

Age Group Victimization Survey

Age Group	Frequency	Percent	Valid Percent
18-34	16	12.8	12.8
35-50	48	38.4	38.4
51-65	18	14.4	14.4
Over 65	40	32.0	32.0
Other/Error	3	2.4	2.4
Total	125	100.0	100.0

Pearson's R, which is also called correlation coefficient, was used to determine if any relationship exists between the dependent and the independent variables. It was the intent of the researcher to determine if a relationship exists between race/gender/ education/etc. and general knowledge of identity theft and identity theft best practices. Recall that Pearson's formula measures the linear relationship of the variables and is symmetric. Ideally, race/gender/education/etc. would have some sort of relationship, either positive or negative, with perceived knowledge of identity theft in the middle Tennessee area. Pearson's R states that a relationship exists when the resultant numerical value is between -1 and +1 with 0 indicating no relationship. For the purposes of this research project, correlation is determined when values exceed 0.05. The weaknesses of correlation coefficient were discussed in Chapter 3. The following expresses the resultant relationships between the dependent and independent variables.

The first significant correlation was determined when comparing ethnicity and question number two; "Do you know what to do if you are a victim of identity theft?" According to Pearson's R they were significantly correlated with $r\ (123) = .198$, $p < .05$.

This correlation means that at least one of the predetermined ethnic groups (Asian, Black, Hispanic, White, Other) do not know what do to should identity theft occur.

Ethnicity was also significantly correlated ($r(123) = .199$, $p < .05$) to question five; "Do you know what fraud alerts are?" Again, there is evidence that at least one of the predetermined ethnic groups are not familiar with the fraud alert system or the benefits associated with placing a fraud alert on one's credit file.

The next significant correlation according to Pearson's R was discovered when analyzing gender and question number seven; "Do you know that identity theft can affect more than your credit report?" ($r(123) = .244$, $p < .05$). There is evidence suggesting the breakdown between males and females is significant when it comes to understanding that there are several different types of identity theft and that each can affect more than just a credit report.

Question eight asked, "Have you ever reviewed your credit report?" and it showed some significant correlation between age ($r(123) = .227$, $p < .05$), ethnicity ($r(123) = .302$, $p < .05$) and employment field ($r(123) = .180$, $p < .05$). Evidently, there are certain age group(s), ethnic group(s) and employment field(s) where reviewing a credit report is seldom, if ever, done. The following table accurately depicts each documented correlation.

Table 20

Correlations Between Variables

Variable	Identity Theft Question	P-value
Ethnicity	Do you know what to do if you are a victim of identity theft?	.198, $p < .05$
Ethnicity	Do you know what "fraud alerts" are?	.199, $p < .05$
Gender	Do you know that identity theft can affect more than your credit report?	.244, $p < .01$
Age	Have you ever reviewed your credit report?	.227, $p < .01$
Ethnicity		.302, $p < .01$
Employment		.180, $p < .05$

According to the data obtained from the questionnaires there is some degree of correlation among the variables (Gender, Age, etc.) and several of the questions that were presented on the survey (Question #2, #5, #7, & #8). However, it would be a mistake to make conclusions or suggest altering an organization's policy or methods based on this research. There are numerous shortcomings and limitations that need to be addressed and discussed. Many of the study limitations will be discussed in the following chapter; however, it is appropriate to briefly explain some of the limitations of the methods that were used.

Pearson's noteworthy weakness is the fact that beyond providing the correlation it does not offer any explanation as to why any specific correlation exists. Although one can review the data and determine that gender correlates with Question #7 ("Do you know that

identity theft can affect more than your credit report?") one will not understand why unless more research is conducted or unless follow-up questions are asked. Likewise, one cannot determine if the relationship is positive or negative so the need for further research cannot be underestimated.

Additionally, it is important not to draw conclusions based on the sample or the questions because respondents were only given two response options, "Yes" and "No". This is an important limitation to highlight because although any two respondents may answer a given question the same way they may have vastly different "levels" of knowledge. Respondents were only given two response options in order to simplify the study and to make it more appealing. An alternative would have been to provide a range of response options for each respondent (i.e. Likert Scale) which would have likely provided greater insight into his or her "knowledge of identity theft". The concept of using simplified, non-descript data is called non-parametric statistics and, although it is considered less powerful, it adequately showed some of the relationships between the variables and the survey questions and highlights the areas where further research is needed.

CHAPTER V: CONCLUSIONS

This research project attempted to determine how knowledgeable a random group of people from a specific geographical region were in regards to identity theft. Though small, this study has potential merit in establishing future research parameters in the study of identity theft and ways to show consumers how to avoid it. The following is a brief synopsis of the strengths and shortcomings of this study as well as any adjustments that may have improved the overall result. Also included is an analysis of like-minded studies and how each compares to this study.

One key element that any future researcher will need to overcome is the level of participation. Considering the methodology of this study there is little that could have been done differently to increase the return rate, though this is something that must be considered when evaluating different research methods as human participation will always be a variable that is difficult to predict or overcome. Voluntary participation research has the potential of being ignored, even though the survey required simple responses and included a self addressed and stamped envelope, only a 34% response rate was received. This is poor given the fact that the survey came from a large, local university and the selected area's relatively high rate of college education. When using a survey it is preferable to have a high return rate as some surveys are incorrectly completed, get lost, or are received by someone who may not speak English or be able to read. A high return rate is preferable to increase the amount of data, enhance the analysis of that which is being studied and more accurately reflect the larger public's perceptions and opinions.

There are few things that could have been done differently to increase the amount of returned surveys but one method that was researched involved obtaining an email

distribution list; however, that may have excluded those who do not own a computer and regularly check their email. It was determined that emailing the survey would have negatively impacted the randomness of the sample and an email distribution list can be very expensive. Furthermore, email addresses can be anonymous and there is a high likelihood that an emailed survey would be sent to a Spam folder or immediately deleted. It is unknown if emailing the survey would have actually increased the return rate by a measurable amount. Another option would have been to distribute the surveys at an event or location where large groups of people gather such as a church, sporting event, concert or shopping mall. This method is convenient and inexpensive but it is not random and surveying from such a venue may have skewed any locality analysis. Utilizing the postal system means recognizing that even though most people receive mail at their residence many homeowners/tenants also receive a large volume of junk mail each year and have become conditioned to discard anything that is not a bill or a check. In sum, there are two concerns a researcher must overcome when conducting research of a similar nature – 1) obtaining a random distribution and 2) the degree of participation.

It is recommended that any future researcher increase the sample size. In order to overcome poor participation rates, distribution limitations, and increase the amount of usable data. Increasing the amount of usable data for statistical analysis would be beneficial for the end result and increase the study's viability. The middle Tennessee area is a mostly homogenous area so any national or even regional assumptions regarding the results are speculative as the sample size is too small and the correlations too insignificant to draw conclusions about a larger portion of the population. One of the correlations exposed by this study is the relationship between knowledge of identity theft best practices and ethnicity;

however it would be a mistake to suggest all ethnic groups are in some way limited in their knowledge of identity theft best practices. Making assumptions or adjusting policy based on the implications gathered from a study of this nature is imprudent as the sample size is very small and the questions could be considered leading. There is also no way to know a respondent's true feelings beyond the "yes/no" options.

In an effort to increase participation and simplify the data analysis, the questions were kept simple, distributed in a similar format, and only provided two possible response options. Although the research did highlight some correlations, they should not be blindly accepted as there are several variables that may have contributed to the results. Some of the questions were leading and could have pushed a respondent toward either an affirmative or negative answer. For example, question six asks, "Do you know there are different types of identity theft?"; this question is worded in such a way as to lead the respondent toward a "yes" response even though previously the respondent may not have known there were different types of identity theft.

In addition to leading respondents to what could be considered the right answer, research that involves human subjects also has the potential to be distorted if each respondent is not completely honest. Question 10 asks "Do you regularly review your bank, credit card and utility statements?" Although this question does not lead a respondent to a right or wrong answer it requires honesty and it is difficult to determine if someone is being honest or if they are choosing to answer in the affirmative because they know its how a responsible person acts. It is recommended that any future research not only include a better gauge, such as a Likert scale, to determine respondent's knowledge but also follow-up questions to determine if the answers are truthful and accurate. In order to accurately gauge someone's knowledge

of identity theft, a researcher should provide a combination of multiple choice questions and a section that asks each respondent to define certain terms or actions. However, this is unrealistic unless one is able to compensate those involved in the study.

The shortcomings of this study are acknowledged in the above paragraphs and it has been determined that increasing participation and the amount of data, addressing distribution shortcomings, and the nature of the survey questions are all areas where a future researcher will need to make adjustments in order to improve this study. This project highlighted the need for more study and for those that completed the survey it may have increased their awareness of identity theft and ways to reduce their risks.

Although the author is not aware of any other studies that duplicate the procedures used here there are numerous studies that have had similar goals and sought to better understand consumer's knowledge of identity theft and how to protect one's identity. The Federal Trade Commission has surveyed individuals repeatedly and provided an avenue online for consumers to report their experiences with identity theft. Although the FTC website provides a way for consumers to report how they were victimized, explains ways to address an identity theft issue, and how to protect one's identity it does not request information about, or maintain a survey database regarding, a consumer's knowledge of best practices or prior behavior. Similarly, the Uniform Crime Report (UCR) and the National Crime Victimization Survey (NCVS) is a compilation of crimes reported in the United States and is maintained by the FBI and the Dept. of Justice respectively but neither addresses an individual's prior knowledge or ways to prevent identity theft. In 2010, the Bureau of Justice Statistics released a supplemental identity theft study from data collected in 2008 that had been conducted along with the NCVS but it too did not address the area of prior knowledge

or best practices. The supplemental identity theft survey would be a good vehicle to conduct attitudinal research as it surveyed 56,480 individuals. Future research, whether by the Dept of Justice or private organizations, should consider including survey questions about a respondent's prior behavior and knowledge of identity theft best practices so as to get a better idea of the public's knowledge.

There is one study that was found to be similar to this one; Identity Theft Awareness in North Central West Virginia was completed in 2003 by G. L. Goodrich for Marshall University in West Virginia. Besides the obvious geographical differences, the methodology and analysis of the data are very dissimilar. In her work, Goodrich (2003) sought to survey various groups of individuals about their knowledge of identity theft but, unlike this study, she utilized several convenience samples and she did not ask about knowledge of identity theft best practices. Goodrich found that the majority of her sample did have at least some knowledge of identity theft and she was able to conclude that she also needed to enlarge the size of her sample. The methodology used by Goodrich was also different in that she was not looking for correlations or trying to tie identity theft knowledge to any demographic information and her analysis did not utilize SPSS or Pearson's R. Goodrich did however provide good insight as far as obtaining a random sample and how best to craft survey questions.

This Identity Theft Risk Assessment of Middle Tennessee provides the reader with a detailed analysis of identity theft and what to do should the crime occur. The middle Tennessee area is known for its culture and is becoming a growing, diverse community that can benefit from increased awareness of identity theft and identity theft best practices. This study thoroughly explains why identity theft awareness is pertinent given the state of the

economy and the lackluster employment sector. Identity theft is no longer a new crime and it will be a problem for the foreseeable future. This is especially true given the advance of the information age and the reliance on our digital footprint in identifying ourselves and our "credit-worthiness". In a speech he gave at a security conference in 2011, Frank Abagnale a fraudster turned security consultant and main character in the major motion picture *Catch Me If You Can* explains that, "People need to be more aware and educated about identity theft. You need to be a little bit wiser, a little bit smarter and there's nothing wrong with being skeptical. We live in a time when if you make it easy for someone to steal from you, someone will".

REFERENCES

Aaron, K., & Schwellenbach, N. (2009, July 10). Mortgage Fraud Reports Rise, But Some Fraud May Still be Undetected. The Center for Public Integrity. Retrieved from http://www.publicintegrity.org/blog/entry/1555/

Baxter, B. (2009, January 22). Kroll Report: Fraud Will Rise as Economic Crisis Deepens. *The AM Law Daily*. Retrieved from http://amlawdaily.typepad.com/amlawdaily/2009/01/kroll-report-says-fraud-to-rise-as-economic-crisis-deepens.html

Biegelman, M. (2009). Identity Theft Handbook: Detection, Prevention and Security. Hoboken, NJ: Wiley & Sons Incorporated.

Crutsinger, M. (2010, April 20). IMF Trims Estimate of Losses from Financial Crisis. ABC News. Retrieved from http://abcnews.go.com/Business/wireStory?id=0423369

Field, A. (2009). Discovering Statistics Using SPSS. London, UK: SAGE Publications Ltd.

Finklea, K. (2012, February 15). Congressional Research Service. Identity Theft: Trends And Issues. Retrieved from http://www.fas.org/sgp/crs/misc/R40599.pdf

Goodrich, G. L. (2003). Identity Theft Awareness in North Central West Virginia. (Unpublished master's thesis). Marshall University, Huntington WV.

Greenberg, A. (2010, September 28). Consumers Are Ditching the $2.4 Billion ID Theft Protection Market. *Forbes* Retrieved from http://blogs.forbes.com/andygreenberg/2010/09/28/consumers-are-ditching-the-2-4-billion-id-theft-protection-market/

Hilsenrath, J., Ng, S., & Paletta, D. (2008, September 18). Worst Crisis Since 30's, With No EndYet in Sight. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB122169431617549947.html

Lanford, J. & Lanford, A. (2007). The College Students Guide to Identity Theft. Scambusters. Retrieved from http://www.scambusters.org/identitytheft/collegestudentsguide.html

Leonard, S. & McClure, M. (2004). Myth and Knowing: An Introduction to World Mythology. New York, NY: McGraw-Hill.

Martin, G. (unknown date). Identity Theft. The Phrase Finder. Retrieved from http://www.phrases.org.uk/meanings/identity-theft.html

Poneman, L. (2009). Fourth Annual US Cost of Data Breach Study. Traverse City, MI: The Poneman Institute. Retrieved from http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf

Poulsen, K. (2010, March 19). Unprecedented 25-Year Sentence Sought for TJX Hacker. *Wired.* Retrieved from http://www.wired.com/threatlevel/2010/03/gonzalez-gov-memo/

Reckard, E., & Menn, J. (2008, August 2). Insider stole Countrywide applicants' data FBI alleges. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2008/aug/02/business/fi-arrest2

Rumsey, D. (2011). *Statistics for Dummies.* Hoboken, NJ: Wiley & Sons Incorporated.

Siciliano, R. (2011, March 23). Identity Theft Ring Operates from Federal Prison. *McAfee Blog Central*. Retrieved from http://blogs.mcafee.com/consumer/identity-theft/identity-theft-ring-operates-from-federal-prison

Starbuck-Gerson, E., & Woolsey, B. (2009). The History of Credit Cards. Austin, TX: Retrieved from http://www.creditcards.com/credit-card-news/credit-cards-history-264.php

Starkman, J. (2013, January 13). E-Filing and the Explosion in Tax-Return Fraud. *Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424127887323374504578222130665022160

Unknown author (2007, June 19). The History of Credit. Retrieved from http://ficoforums.myfico.com/t5/Understanding-FICO-Scoring/The-History-of-Credit/td-p/19935

Unknown author (2009). Identity Theft Statistics. SpendonLife. Retrieved from http://www.spendonlife.com/guide/2009-identity-theft-statistics

Unknown author (2008). Javelin Strategy & Research Report. Retrieved from http://www.identitytheft.com/article/theft_vs_fraud

Unknown author (2005). Working to Resolve Identity Theft. Identity Theft Resource Center. Retrieved from http://www.idtheftcenter.org/

Unknown author (2003, September 1). Identity Theft Surveys and Studies: How many identity theft victims are there? What is the impact on victims?. Privacy Rights Clearinghouse. Retrieved from http://www.privacyrights.org/ar/idtheftsurveys.htm

Unknown author (n.d.). Punishment for Identity Theft. Identity Management Institute. Retrieved from http://www.identity-theft-awareness.com/punishment-for-identity-theft.html

Unknown author (n.d.). Identity Theft Punishment and Penalties, Federal and State Laws. Retrieved from http://www.identitytheft.com/article/idenity _theft_punishment

Unknown author (2009, January 21). Fraud Set to Rise as Financial Crisis Deepens. *All Business*. Retrieved from http://www.allbusiness.com/company-activities-management/company-structures/11755895-1.html

Vijayan, J. (2007, March 29). TJX data breach: At 45.6M card numbers, it's the biggest ever. *Computerworld*. Retrieved from, http://www.computerworld .com/s/article/ 9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever

Internet Crime Complaint Center (2009). Annual Report. Retrieved from http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

Impulse Research Corp (2002). College Students Risk Factors study conducted for the Chubb Group Insurance Company. Retrieved from http://www.scambusters.org/ identitytheft/collegestudentsguide.html

Identity Theft & Credit Fraud. (n.d.). Retrieved from http://www.identitytheftcreditfraud .com/index.htm.

Nucleus Research (2004). Spam – The Serial ROI Killer. [Report E50]. Retrieved from http://nucleusresearch.com/research/notes-and-reports/spam-the-serial-roi-killer/

Privacy Rights Clearinghouse. (n.d.). Retrieved from http://www.privacyrights.org/

Federal Reserve Bank of St. Louis. (n.d.). The Financial Crisis; A Timeline of Events And Policy Actions. Retrieved from http://timeline.stlouisfed.org/index .cfm?p=timeline

Federal Trade Commission (n.d.). *Fighting Back Against Identity Theft*. Retrieved from http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html

Federal Trade Commission (2012). Identity Theft Tops List for 13th Consecutive Year in Report of National Consumer Complaints. Retrieved from http://www.ftc.gov /news-events/press-releases/2013/02/ftc-releases-top-10-complaint-categories-2012

US Citizenship and Immigration Service (n.d.). *History and Milestones*. Retrieved from http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a 3e5b9ac89243c6a7543f6d1a/?vgnextoid=84979589cdb76210VgnVCM100000b92ca 60aRCRD&vgnextchannel=84979589cdb76210VgnVCM100000b92ca60aRCRD

USPS Annual Report. (2007). Retrieved from http://postcom.org/eco/sls.docs/USPS-Annual%20Report%202007.pdf

US Census Bureau. (2010). Williamson County, Tennessee. Retrieved from http://quickfacts.census.gov/qfd/states/47/47187.html

U.S. Department of Justice. (n.d.). *Identity Theft & Identity Fraud*. Retrieved from http://www.justice.gov/criminal/fraud/websites/idtheft.html

U.S. Department of Justice Bureau of Justice Statistics. (n.d.). *Identity Theft*. Retrieved from http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=42

U.S. Department of Justice. (n.d.). *Office of Justice Programs: Identity Theft*. Retrieved from http://www.ojp.usdoj.gov/programs/identitytheft.htm

U.S. Department of Justice National Drug Intelligence Center. (2007).

Retrieved from http://www.justice.gov/ndic/pubs22/22972/index.htm

APPENDICES

Appendix A

July 22, 2011

Craig Moore
Department of Criminal Justice
craigmoore7@gmail.com, dpowell@mtsu.edu

Protocol Title: "Identity Theft Risk Assessment in Middle TN"

Protocol Number: 12-004

Dear Investigator(s),

I found your study to be exempt from Institutional Review Board (IRB) continued review. The exemption is pursuant to 45 CFR 46.101(b) (2). This is because your study involves the use of survey materials, and the information was recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects.

You will need to submit an end-of-project report to the Office of Compliance upon completion of your research. Complete research means that you have finished collecting data and you are ready to submit your thesis and/or publish your findings. Should you not finish your research within the three (3) year period, you must submit a Progress Report and request a continuation prior to the expiration date. Please allow time for review and requested revisions. Your study expires on **July 22, 2014.**

Any change to the protocol must be submitted to the IRB before implementing this change. According to MTSU Policy, a researcher is defined as anyone who works with data or has contact with participants. Anyone meeting this definition needs to be listed on the protocol and needs to provide a certificate of training to the Office of Compliance. **If you add researchers to an approved project, please forward an updated list of researchers and their certificates of training to the Office of Compliance before they begin to work on the project.** Once your research is completed, please send us a copy of the final report questionnaire to the Office of Compliance. This form can be located at www.mtsu.edu/irb on the forms page.

Also, all research materials must be retained by the PI or **faculty advisor (if the PI is a student)** for at least three (3) years after study completion. Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,
Emily Born
Compliance Officer
615-494-8918
eborn@mtsu.edu

Appendix B

Department of Criminal Justice
1421 East Main St.
Murfreesboro, TN 37132

Greetings from Nashville, Tennessee; my name is Craig Moore and I am studying criminal justice at Middle Tennessee State University.

I am contacting you because you have been selected at random to complete the attached survey.

I am surveying individuals in the middle Tennessee area regarding identity theft. The FBI has labeled identity theft as the fastest growing crime in America and it affects millions of Americans each year. It is hoped that the information learned through this survey will assist in greater consumer awareness and help reduce identity theft crime.

Please take a few moments to complete this survey and return it in the attached envelope. In order to keep this survey anonymous, please do not write your name on any correspondence. Your participation is very much appreciated.

Thank you,

Craig Moore

Appendix C

Identity Theft Knowledge Survey

(Please circle the appropriate response number)

Your participation in this survey is voluntary and anonymous. You must be 18 or older to participate and all information will be kept confidential. Thank you for taking the time to complete this survey.

Gender: 1).Male 2).Female
Age Group: 1).18-28 2).29-39 3).40-50 4).51-61 5).62-72 6).73-83 7).84-94
Ethnicity: 1).Asian 2).Black 3).Hispanic 4).White (non Hispanic) 5).Other
Highest Level of Education: 1).High School/GED 2).Associates Degree 3).Bachelors Degree 4).Masters Degree 5).Post Graduate Degree 6).None of the above
Employment: 1).Clerical 2).Construction 3).Professional 4).Law Enforcement 5).Sales 6).Service Industry 7). Retired 8).Other (Please specify _____)

---

1). Do you know what identity theft is? 1).Yes 2).No

2). Do you know what to do if you are a victim of identity theft? 1).Yes 2).No

3). Do you know someone who has been a victim of identity theft? 1).Yes 2).No

4). Have you been a victim of identity theft? 1).Yes 2).No

5). Do you know what "fraud alerts" are? 1).Yes 2).No

6). Do you know there are different types of identity theft? 1).Yes 2).No

7). Do you know that identity theft can affect more than your credit report? 1).Yes 2).No

8). Have you ever reviewed your credit report? 1).Yes 2).No

9). Have you reviewed your credit report in the last six months? 1).Yes 2).No

10). Do you regularly review your bank, credit card and utility statements? 1).Yes 2).No

11). Do you shred documents that contain your personal or financial information? 1).Yes 2).No

12). Do you take steps to reduce the likelihood of identity theft? 1).Yes 2).No

13). Can information on credit reports be used for employment hiring purposes? 1).Yes 2).No

14). Select the age group that you think is most often victimized by identity theft.
1).18-34
2).35-50
3).51-65
4).Over 65