1-1-2003

Identity Theft Awareness in North Central West Virginia

Gwendolyn Lea Goodrich

IDENTITY THEFT AWARENESS IN NORTH CENTRAL WEST VIRGINIA

Thesis submitted to
Marshall University

In partial fulfillment of the
Requirements for the degree of
Master of Science
Criminal Justice

by

Gwendolyn Lea Goodrich

Dr. Deanna Shields, Committee Chairperson
Dr. Elaine Bartgis
Dr. Margaret Phipps Brown, Thesis Coordinator

Marshall University

April 2003

ABSTRACT

"IDENTITY THEFT AWARENESS IN NORTH CENTRAL WEST VIRGINIA"

By Gwendolyn Lea Goodrich

Identity theft occurs when an individual "takes over" the identity of another without that person's consent or when someone uses bits and pieces of information about an individual to represent himself or herself as that person for fraudulent purposes. The simplicity of gathering personal identification through technology enhancements has made identity theft reportedly the fastest growing crime in the U.S. The latest report indicates, through a national survey, that 20 percent of Americans are victims of identity theft. However, the impact of this growing crime has not been assessed in North Central West Virginia, where this study occurred. The theory is that, even with colleges and a federal law enforcement agency in the area, the majority of residents do not know about identity theft or what to do if they are victimized. Through this study, however, it was determined that the residents of this area are mostly aware of identity theft and what to do if they are victimized.

DEDICATION

The author wishes to dedicate this thesis to the family and friends who supported her through her two years in the program leading to this product.

ACKNOWLEDGMENTS

The author wishes to acknowledge several people, without whom this would not be possible. First and foremost, to the teachers at Fairmont State College and Marshall University, specifically Dr. Peggy Brown, Dr. Deanna Shields, Dr. Elaine Bartgis, Dr. Fred Fidura, and Dr. Chuck Shields, who worked through the seemingly impossible task of coordinating class schedules with her work schedule, particularly when extensive travel occurred. Next, she would like to thank her family, especially her parents and grandmother, for their love and support throughout her entire life and particularly during the past two years. Finally, she wants to thank her friends and co-workers for their constant encouragement to complete this degree.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER I

Introduction

Identity Theft Awareness In North Central West Virginia

Identity theft occurs when an individual "takes over" the identity of another without that person's consent or when someone uses bits and pieces of information about an individual to represent himself or herself as that person for fraudulent purposes (Givens, 2000). Identity theft is not a new crime. News reports as early as 1985 provided advice to individuals on how to protect themselves from identity theft. Since then, the simplicity of gathering personal identification through technology enhancements has made identity theft reportedly the fastest growing crime in the U.S. The latest report indicates through a national survey that 20 percent of Americans have been victims of identity theft (Survey: 1 in 5 Americans victimized by ID theft, 2003). New bills are currently being introduced in Congress to support stronger, harsher penalties on perpetrators and to provide more assistance to the victims. In January 2003, the Federal Trade Commission stated that complaints of identity theft doubled in 2002 (Federal Trade Commission [FTC], 2003). Privacy groups report that over 750,000 Americans will fall victim to identity theft scams through credit card fraud and account takeovers. However, the impact of this growing crime has not been assessed in North Central West Virginia, where the study for this thesis occurred. The theory is that, even with colleges and a federal law enforcement agency in the area, the majority of residents do not know about identity theft or what to do if they are victimized.

The completion of this thesis is two-fold: an extensive review of the literature was conducted as it pertains to the overall problem of identity theft, and surveys were issued to students at Fairmont State College (FSC) and employees of a federal law enforcement agency to obtain their knowledge about identity theft. Information for the review of the literature was obtained and reviewed from the Federal Bureau of Investigation, U.S. Secret Service, U.S. Postal Service, Internal Revenue Service, Federal Trade Commission, Internet Fraud Complaint Center, the General Accounting Office, and other regulatory and investigative agencies to determine the current extent of identity theft investigations. Additionally the proposed legislation and its potential impact on the identity theft problem were explored, and newspapers in the United States and abroad where identity theft is frequently occurring were reviewed.

CHAPTER II

Review of Literature

Background of Identity Theft and Laws Pertaining to Identity Theft

Background

As previously stated, identity theft occurs when an individual "takes over" the identity of another without that person's consent or when someone uses bits and pieces of information about an individual to represent himself or herself as that person for fraudulent purposes (Givens, 2000). Identity theft primarily takes two forms: "true name fraud" and "account takeover." True name fraud occurs when someone uses a consumer's personal information to open new accounts in his or her name. Account takeover occurs when criminals gain access to a person's existing accounts and make fraudulent charges (National White Collar Crime Center [NW3C], 2001).

Identity theft is investigated as a white-collar crime. Over 60 years ago, criminologist Edwin Sutherland coined the term “white collar crime.” In his theory "White Collar Criminality," Edwin Sutherland stated that "the financial cost from white collar crime is probably several times as great as the financial cost of all the crimes which are customarily regarded as the 'crime problem'. . . white collar crime is real crime" (Sutherland, 1940, p.6).

Identity thieves use a variety of ways to obtain personal or financial information about their victims. Generally, they obtain a name, Social Security number, credit card number, or date of birth through various sources. Some of the most "old fashioned" ways of stealing identifying information are by stealing a wallet or a purse, or "dumpster diving," which involves rifling through the victim's trash to obtain credit card slips, bank statements, or credit applications

(Givens, 2000). Once the criminals have this information in hand, they can do a change of address form to divert the victim's account information to a new mailing address, or they can apply for the "pre-approved" credit in the victim's name and change the address, so that they receive the cards and statements, leaving the victim totally unaware of the situation (FTC, July 2001).

There has been an increase in the "inside job" identity thief, where a dishonest employee with access to personal and financial information of many other individuals, either through bank records or the credit reporting agencies (Givens, 2000). Sometimes these individuals do not commit the identity theft themselves; rather, they sell this information to anyone willing to pay for it (FTC, July 2001).

Some identity theft is perpetrated by relatives or friends, roommates, household workers, and spouses going through a divorce who have a grudge. Due to their close relationships with the victims, these individuals have easy access to Social Security numbers, driver's license numbers, and credit card numbers (Givens, 2000). Other times, identity thieves fraudulently obtain the victim's credit report by posing as a landlord, employer, or someone else who may have a legitimate need for, and a legal right to, the information (Givens, 2000).

Other techniques include "shoulder surfing" and "eavesdropping." Shoulder surfing occurs when someone looks over a potential victim's shoulder to gain personal information. For example, when a check is written at the grocery store or a PIN number is entered in the Automated Teller Machine (ATM), a shoulder surfer tries to obtain personal information from the victim. Eavesdropping takes place when the victim gives credit card information or telephone calling card numbers over the telephone while the criminal "listens in" (NW3C, 2001).

Finally, the Internet offers personal information about potential victims to just about anyone. An example is the case of Abraham Abdallah, a busboy in New York who, when arrested in March 2001, had Forbes magazine's issue on the 400 richest people in America, plus Social Security numbers, credit card numbers, bank account information, and mother's maiden names for intended victims including Steven Spielberg, Oprah Winfrey, and Martha Stewart. Abdallah was accused of using websites, e-mail, and off-line methods to try to steal the identities of celebrities and make off with millions in assets. One scheme allegedly involved sending an e-mail purporting to come from Siebel Systems founder Thomas Siebel to Merrill Lynch, directing that $10 million be transferred to an offshore account (Cohen, 2001).

Once criminals gain access to personal and financial information, the actual identity theft begins. Criminals use this information in many ways, varying from writing bad checks to creating criminal records.

A name, Social Security number, and driver's license are basically all that is required to open a checking account. Armed with this knowledge, identity thieves open an account and write bad checks on it. Additionally, with a date of birth, criminals can open new credit card accounts, use the cards to the maximum limit, and allow the account to become delinquent by not paying the bills. If the criminal obtains a current credit card number, he or she will use it for purchases. Criminals also call the issuing card agency and request a change of address. Since the bill is sent to the new address, the victim is unaware of the purchases, or the fact that the account is delinquent. These accounts are then reported on the victim's credit report. Sometimes, identity thieves file for bankruptcy under the victim's name to avoid paying debts they have incurred (FTC, July 2001).

Criminals also establish utilities under victims' names, including telephone or wireless service, which can also be reported to the credit reporters as delinquent if not paid. According to the Federal Trade Commission, unauthorized phone or utility services accounted for 21 percent of the identity theft complaints received from November 1999 through June 2001. New wireless service comprised 42 percent of these complaints, while new telephone service accounted for an additional 33 percent (FTC, June 2001).

In extreme cases, identity thieves use their victim's information to obtain loans or employment benefits, or even commit crimes. Some identity thieves buy cars or take out auto loans in their victims' names, while others apply for and receive business loans or student loans for school. Some use their victims' Social Security number to apply for jobs or to work. Finally, some identity thieves may give a victim's name if they are arrested for committing a crime, such as burglary, robbery, driving under the influence, or even murder. This may create a fraudulent criminal record, which can take a long period of time to clear (FTC, July 2001).

<u>Laws</u>

Identity theft can be federally prosecuted under the Identity Theft and Assumption Deterrence Act of 1998 (The Identity Theft Act), 18 U.S. Code § 1028. This law prohibits anyone from knowingly transferring or using, without lawful authority, someone else's "mean(s) of identification" with the intent to commit, aid or abet, any unlawful activity that constitutes a violation of federal law or that constitutes a felony under state or local law. The law allows for sentences of up to 15 years imprisonment and a substantial fine for any person committing the offense who, as a result of the offense, obtains anything worth $1,000 or more during any one-year period. Since 1998, federal prosecutors have initiated more than 100 federal criminal prosecutions for identity theft (Rusch, 2001). New legislation, proposed by Senator Diane Fienstein of

California, is currently under review in the Senate. This law would increase sentencing for identity theft offenses and provide more protections for victims and citizens, including a free copy of a credit report each year.

Identity theft is investigated by several federal agencies, including the U.S. Secret Service (USSS), Federal Bureau of Investigation (FBI), Federal Trade Commission (FTC), Social Security Administration-Office of Inspector General (SSA-OIG), Internal Revenue Service-Criminal Investigative Division (IRS-CI), and the U.S. Postal Service Inspection Division (USPIS), as well as state and local law enforcement. While the Identity Theft Act of 1998 created a federal violation for this crime, 43 states have enacted specific identity theft laws. Currently, under many of these state laws, identity theft is a misdemeanor (Givens, 2000). The West Virginia State code for addressing identity theft is §61-3-54:

> **Taking identity of another person; penalty.**
>
> Any person who knowingly takes the name, birth date, social security number or other identifying information of another person, without the consent of that other person, with the intent to fraudulently represent that he or she is the other person for the purpose of making financial or credit transactions in the other person's name, is guilty of a felony, and upon conviction, shall be punished by confinement in the penitentiary not more than five years, or fined not more than one thousand dollars, or both: *Provided*, That the provisions of this section do not apply to any person who obtains another person's drivers license or other form of identification for the sole purpose of misrepresenting his or her age (West Virginia Legislature, n.d.).

Identity Theft Statistics

Credit card fraud is the most frequently reported scheme related to identity theft. Between November 1999 and June 2001, the FTC received over 30,000 complaints of credit card fraud facilitated through identity theft. These complaints included true name and account takeover. New accounts were opened in the victims' name in 66 percent of the reports (Keeping count with ID theft, 2001).

Victims had a relationship with their offender in 12 percent of the identity thefts reported to the FTC (FTC, June 2001). Relationships that were identified included family members; roommates/co-habitants; neighbors, workplace co-worker, employer, or employee; or other unknown, such as individuals working in the victim's home. Approximately fifty percent of the known victims reported were family members (US General Accounting Office [GAO], 2002).

There are no comprehensive statistics on the prevalence of identity theft or identity fraud. According to the consumer reporting agencies (Experian, Equifax, and TransUnion), the most reliable indicator of the incidence of identity theft is the number of seven-year fraud alerts placed on consumer credit files. A fraud alert is a warning placed on the credit file of an identity theft victim by a credit reporting agency to prevent further credit from being established without the verbal consent of the victim. These alerts are on file from between one and seven years (US GAO, 2002). The three credit reporting agencies reported significant increases in the number of alerts placed on file from 1999 to 2000, ranging from 36 percent to 53 percent (Stana, 2002).

At the end of 2000, the financial services industry incurred costs at close to $2.5 billion due to identity theft. Costs from identity theft fall into several categories, with direct losses from the fraud itself accounting for 48 percent. Other costs associated with identity theft include additional staff and training and the implementation of new technology (Lee, 2001). Financial institutions filed 352 suspicious activity reports relating to identity theft between December 1, 2000, and June 30, 2001, a 50 percent increase from the same period a year before. In a report to the US General Accounting Office (1998), the American Bankers Association claimed that check fraud-related losses attributable to identity theft in 1999 was reported mostly by superregional/money center banks, i.e. those with assets of $50 billion or more. The superregional banks reported 65 percent of their check fraud losses were impacted by identity theft. Community banks, which have assets of under $500 million, comprise the majority of the banks nationwide. These banks reported 10 percent losses as a result of identity theft. Mid-size banks, those with between $500 million and under $5 billion, and regional banks, those with assets between $5 billion and under $50 billion, reported a total of 43 percent of all check fraud losses due to identity theft (US GAO, 1998).

In the report *National and State Trends in Fraud and Identity Theft, January-December 2002,* the FTC reported that they received 161,819 complaints of identity theft in Calendar Year 2002. The FTC also provided demographic information about reported victims of identity theft. According to the FTC, 75 percent of the complainants were between the ages of 18 and 49. Nearly half (49 percent) of the victims were between the ages of 30 and 49. Reports of identity theft were made from all 50 states and the District of Columbia. The largest numbers of complaints were collected from the District of Columbia, California, Arizona, Nevada, and Texas. West Virginia reported only 360 complaints in 2002, ranking 47th out of 51 areas. The cities in West Virginia reporting the most identity thefts were Charleston, Parkersburg, Huntington, Morgantown, and Beckley (FTC, 2003).

The FBI had a total of 7,694 Financial Institution Fraud (FIF) cases pending as of June 11, 2002. Of this total, 209 cases, or 2.72 percent, involved identity theft. Additionally, the FBI reported that nearly 1,000 cases in other criminal investigations involved identity theft. These cases include wire fraud, credit card fraud, and use of fraudulent documents (FBI, 2002).

The FBI also reported statistics from the Internet Fraud Complaint Center (IFCC), which is a joint venture between the National White Collar Crime Center and the FBI. The IFCC refers complaints of Internet fraud to federal, state, and local law enforcement for investigation. According to the IFCC annual report for 2001, identity theft accounted for 1.3 percent of the 16,775 complaints that were referred from IFCC in Calendar Year 2001. These complaints were referred to the USSS and the FTC. The average dollar loss per complaint was $3,000, based on reports from 22.8 percent of identity theft complainants (NW3C and FBI, 2001).

Another agency actively investigating identity theft is the United States Postal Inspection Service (USPIS). The USPIS recorded a 36 percent increase in identity theft-related arrests between 1996 and 2001. In 1996, the USPIS arrested 1,287 individuals involved with identity theft; that figure rose to 1,752 by June 30, 2001 (US GAO, 2002).

The Social Security Administration Office of Inspector General (SSA-OIG) operates a hotline, which receives allegations of fraud, waste, and abuse. In recent years, the hotline staff recorded allegations involving identity theft as either Social Security number (SSN) misuse or program fraud, which contained elements of SSN misuse. Allegations of SSN misuse include incidents wherein a criminal used the SSN of a victim for the purpose of fraudulently obtaining credit, establishing utility services, or acquiring goods. In Fiscal Year (FY) 1998, the SSA/OIG hotline received a total of 25,600 calls related to SSN misuse and program fraud. By FY 2001, the calls related solely to SSN misuse had increased to 65,220. Calls with allegations of program fraud also increased, to 38,883. In the six-month period between March and September 2001, the hotline received 25,991 complaints alleging SSN misuse that directly involved identity theft. Over 36 percent of these complaints were credit card fraud (US GAO, 2002).

The Internal Revenue Service Criminal Investigative Division (IRS-CI) investigates cases of identity theft related to questionable federal tax refund schemes. In some instances, false returns are filed by the true taxpayer using false income documents with inflated income and/or withholdings. The IRS does not keep statistics documenting the number of questionable returns involving identity theft or identity fraud. However, the IRS did compile statistics regarding questionable refunds that involved a "high frequency" of identity theft or identity fraud for the March 2002 GAO report. In 1996, the IRS-CI investigated 2,458 questionable refund schemes involving $82 million in fraudulent refunds claimed. By Calendar Year 2000, the IRS detected 3,085 questionable refunds totaling $783 million (US GAO, 2002).

Victims Rights and Experiences

Victims of identity theft often experience non-monetary harm in addition to financial losses. The leading types of non-monetary harm cited by victims were "denied credit or other financial services," "invaded privacy," "time lost to resolve problems," and "lack of closure." Some victims also alleged that they had been subjected to "criminal investigation, arrest, or conviction." According to a May 2000 report from the California Public Interest Research Group and the Privacy Rights Clearinghouse, identity theft victims spent 175 hours, on average, trying to resolve their identity-theft related problems (Stana, 2002). Victims also alleged that: (1) they got little to no help from the authorities who issued the identifying information to them; (2) that law enforcement did not investigate many identity theft crimes because there are too many complaints; and (3) that they did not get effective help from the credit grantors, banks, or the credit reporting agencies (Givens, 2000).

While most financial institutions do not hold victims liable for fraudulent debts, victims may incur significant expenses trying to restore their good names and financial health. The FTC reported that, routinely, victims incur costs for document copies, notary fees, certified mail, and long-distance telephone calls. Some victims have even had tax refunds or other benefits withheld pending resolution of the identity theft crime. Not counting legal fees, victims reported spending between $30 and $2,000 on costs related to their identity theft. The average reported loss directly incurred as a result of the identity theft was $808, but most victims estimated spending an additional $100 for out-of-pocket costs while trying to restore their credit (US GAO, 2002).

Fortunately, the victims of identity theft do have some protection related to monetary losses. The Truth in Lending Act limits liability for unauthorized credit card charges in most cases to $50 per card. The Fair Credit Billing Act established procedures for resolving billing errors on credit card accounts that include fraudulent charges on the account. To take advantage of the law's protections, victims need to write a letter to the creditor at the address given for "billing inquiries" that includes the victim's name, address, account number, and a description of the billing error, including the amount and date of the error. The letter needs to be sent so that it reaches the creditor within 60 days after the first bill containing the error was mailed out. If the identity thief changed the address on the account and the bill was not received, the dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill or the victim may be responsible for the charges. The letter should be sent by certified mail with a request for return receipt, and the creditor must acknowledge the complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles, but not more than 90 days, after receiving the letter from the victim (FTC, July 2001).

The Fair Debt Collection Practices Act prohibits collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection. A victim of identity theft can stop a debt collector from contacting them by writing a letter to the collection agency telling the agency to stop. Once the letter is received, the company is not to contact the victim again, with two exceptions: to inform the victim that there will be no further contact or to advise the victim that the debt collector or the creditor intends to take some specific action. A collector also may not contact victims if, within 30 days after a written notice is received, the victim sends the collection agency a letter stating that the victim does not owe the money. Although this letter should stop the debt collector's calls, it will not necessarily get eliminate the debt itself, which may still appear on a credit report. Additionally, a collector can renew collection activities if a victim is sent proof of the debt. Because of this, victims are advised to send copies of documentation supporting their position, along with a copy of the filed police report, with the letter to the debt collector (FTC, July 2001).

Protection for transactions involving an Automated Teller Machine (ATM) or debit card or other electronic way to debit or credit an account is provided by the Electronic Fund Transfer Act. This Act also limits the liability for unauthorized electronic fund transfers. The amount of loss that the victim is directly responsible for depends on how quickly the lost or stolen ATM or debit card is reported. If the card is reported lost or stolen within two business days of discovering the loss or theft, the losses incurred by the victim are limited to \$50. If the card is reported after two business days but within 60 days after a statement showing the unauthorized electronic fund transfer is received, the victim can be liable for up to \$500 of the amount or amounts a thief withdraws. If the victim waits more than 60 days, the victim could be liable for all the money that was taken from the account after the end of the 60 days and before the card is reported missing. VISA and MasterCard have voluntarily agreed to limit the victim's liability for unauthorized use of a debit card in most instances to $50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card. The best way for victims to protect themselves in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing with a certified letter, return receipt requested. After notification of an error on a statement, the institution generally has 10 business days to investigate. The financial institution must inform the victim of the results of its investigation within three business days after completing it and must correct an error within one day of determining that an error has occurred (FTC, July 2001).

Many news reports indicate that people everywhere are becoming victimized by identity theft. While the justice system usually focuses on perpetrators, identity theft victims are the focus of this crime in news articles and television interviews. Some of these stories include:

I. Michelle Brown, lacking the money to study beyond high school, took after-school jobs to finance her college education. Establishing credit at 17 and having no problems with the law, she never anticipated what happened to her 11 years later. Someone had stolen her identity, bought a new truck, rang up more than $50,000 in goods and services, and was arrested for trafficking 3,000 pounds of marijuana, all in Michelle’s name. After 500 hours of legwork and pleading with creditors and law enforcement, Michelle has restored her good name, but not without emotional scars. “I faced many difficulties in clearing my name, and I still face the fear that I will forever be linked with the perpetrator’s criminal record” (Del Grosso, 2001).

II. Kevin Reigrut received a letter from Circuit City that prompted him to notify police about a possible identity theft. He learned that someone had used his identity to not only apply for credit at Circuit City, but was entering into a leasing agreement on $60,000 in computer equipment. “It was a systematic car-jacking of my entire identity,” he said. He has since purchased two paper shredders and refuses to allow his license to be photocopied. “This may be one of those prices of being in the Internet age, but it’s certainly not a price worth paying. It’s horrifying” (Biemer, 2002).

III. Anna Mae Dugger, who says she has felt helpless, frustrated, and angry for a year and a half, is finally getting some relief. A woman with a similar name, who had used Dugger’s name, birth date, and Social Security number to run up credit and bills. Upon learning of the perpetrator’s arrest, Dugger responded, “I know who and I know why, what I want to know is how” (Ingram, 2002).

IV. Melissa Marsh, another victim of identity theft, found herself so “devastated” by the experience that she and her husband are selling their secluded mountain home and leaving, but won’t say to where. “I sleep with a .30-.30 next to my bed, afraid that she will come back. I also had visions of her killing us and becoming us–because she had my identity” (Mercury News, 2002).

V. Arlene Tietboehl was more than surprised when she found out her former friend used her identity to run up more than $180,000 in debt. “At first I felt very stupid when it happened, because I was hurt more than anything,” Tietoboehl said. “I cried for weeks.

> We're ecstatic that she was caught. I'm just thankful that they got her and she can't do it to somebody else" (Franceschina, 2002).

Several news columns have been dedicated to identity theft, as the reporters themselves have been victimized. The columnists write about their personal experiences, and the problems they have encountered trying to repair their credit. Associated Press Reporter Nedra Pickler (2002) was a victim. The perpetrator in her case charged $30,000 of merchandise on credit cards in just a week. Pickler said that she was "lucky" to find out about the theft early and she had no idea who the thief was or how the thief got her information. "It used to be thieves broke into homes and took whatever they could as quickly as they could. Good neighbors or a good watchdog could stop them. But identity thieves can shop where they want, when they want and for what they want. And there is nothing neighbors and dogs can do about that."

San Francisco Chronicle writer David Lazarus (2002) wrote two columns about his misfortune and provided information for others who may be victimized to help them. Lazarus never did report how much credit was charged in his name, but he said, "I'll probably never know for sure how this all started. Instead, I have [his] legacy to attend to, a violation of my privacy, and an invasion of my life that will require elaborate efforts to remedy. Just the other day, he was preapproved for a $22,500 car loan if he buys his next car at Serramonte Dodge, Serramonte Mitsubishi, or Serramonte Nissan. I'll let him know next time I see him."

Identity theft is not just a problem in the United States. Two news reporters, from London, England and Australia, also reported identity theft issues in their respective countries. The reporter from London was himself a victim (Watts, 2002), and the report from Australia stated that an estimated 25 percent of all fraud reported to the Australian Federal Police involved false identities, costing Australians more than $4 billion a year. A victim stated about his perpetrator, “He was charged, but I’m not sure if it ever went to court, as it was deemed he had a psychiatric illness. I have no idea what became of him, other than that he was institutionalized for a period of time. . .I’ve stopped dreaming about him now, but I’m not so confident that he’ll never appear again” (Cullen, 2002).

Conclusion

Many more stories of victims are sure to be reported, as the largest identity theft case in American history broke in New York on November 25, 2002. Three men using the identities of at least 30,000 people nationwide racked up over $2.7 million in cash and purchases (U.S. Attorney’s Office, 2002). In Canada, representatives of a life insurance company said that the company would compensate customers who incur out-of-pocket expenses in preventing possible identity theft after the disappearance of a hard drive containing confidential information on 180,000 customers (Flavelle, 2003). Job posting sites, such as Monster.com, have come under pressure for more security as people who may not be valid employers request resumes to obtain individual’s personal identifiers (Keefe, 2003).

With limited statistics and news information about this relatively new crime, a survey was conducted to determine if there has been any impact of identity theft in North Central West Virginia. This survey assessed the awareness of residents regarding laws, available identity theft information, and what to do if victimized.

CHAPTER III

Methods

Research Questions

This survey was designed to answer certain research questions to determine the extent of identity theft awareness in North Central West Virginia. The research questions were directly related to the questions on the survey and are answered through the survey results. The research questions for this study were:

1. Are the respondents more aware of a federal identity theft statute than a West Virginia statute?

2. Do the respondents believe that victims usually know their perpetrators?

3. Do the respondents know what a fraud alert is and who to call to have one placed in a credit file?

4. Have the respondents heard of the Federal Trade Commission?

5. What do the respondents believe criminals do with stolen identifying information, and what do the respondents believe individuals should do if they believe they have become identity theft victims?

6. What do the respondents believe is the most common age of victims?

7. Do the respondents know how many credit reporting agencies exist?

8. Have the respondents been victims of identity theft or know someone who has been a victim of identity theft?

Initial Survey

The Identity Theft Awareness Survey was initially designed and administered as an exploratory study for a research methods class. This pilot study was initially disseminated to 37 law enforcement employees and residents of Jacksonville, Florida in November 2002 (see Appendix A). The respondents were chosen as a convenience sample, as the researcher was assigned in a law enforcement office in Jacksonville, and the researcher conducted a seminar of identity theft awareness at a church in Jacksonville. The survey was disseminated to the meeting attendees before the meeting began and was used for discussion points throughout the evening. The purpose of this Identity Theft Assessment Survey was to obtain qualitative and quantitative data regarding identity theft awareness and to discover problems or issues for the thesis survey.

The exploratory survey consisted of two parts. Part 1 was designed for qualitative purposes and asked for personal experience either as a victim of identity theft or as an acquaintance of someone who was a victim. Only one response was reported to this question. The second part was the quantitative assessment and asked for Yes/No responses or to circle the best answer in a multiple choice setting. The results of this survey were minimal, but showed that the surveyed residents of the Jacksonville area were aware of the identity theft issue and what to do if victimized. A paper of the findings was submitted, along with an oral presentation, for the research methods class in December 2002.

The survey results produced several problems, including some questions left unanswered or multiple answers chosen for one question. Also, no demographic information was requested, so the results could not easily be compared with the known national statistics.

Current Survey

The Identity Theft Awareness Survey used in this study was designed to elicit information about identity theft awareness and reflected the changes indicated by the pilot study. In order to obtain more clear and concise information, this survey (see Appendix B) included requests for demographic information, specified that each question must have only one answer chosen, and provided an "I don't know" response to questions that may have produces false statistics, through guessing, in the previous survey.

As this study pertains to North Central West Virginia, it is important to identify the affected counties and their populations. North Central West Virginia is generally comprised of Monongalia, Marion, Harrison, and Taylor counties. The populations according to the US Census Bureau, for Census 2000, are 68,652 in Harrison County, 56,598 in Marion County, 81,866 in Monongalia County, and 16,089 in Taylor County (US Census, 2003). This totals 223,205 residents within the four county area.

The survey of identity theft awareness asked ten close-answered questions directly related to the subject, five questions for demographic comparisons, and one open-ended "comments" section. The first three questions, "Is identity theft a Federal offense?", "Does West Virginia have a state statute addressing identity theft?", and "Do victims usually know their perpetrators?" provided three responses from which to choose: (1) Yes, (2) No, and (3) I don't know. The next two questions, "Have you ever heard of a 'fraud alert'?" and "Have you heard of the Federal Trade Commission?" required only a Yes or No answer.

The next five questions were multiple choice and offered either four or five possible responses. These questions included, "How do most criminals use the identifying information they have stolen?", "What is the most common age group of identity theft victims?", "How many credit reporting agencies are there?", "Who should victims call to have fraud alerts placed on their file?", and "What should you do if you believe your identity has been stolen?"

The survey was submitted to the Internal Review Board (IRB) for Marshall University in January 2003. A memorandum, stating that the study, as submitted, would be exempt from IRB review and approval was issued on March 12, 2003 (see Appendix C). The surveys were disseminated and collected by the researcher from the FSC students and all but one section of the federal agency. All completed surveys were returned by March 21, 2003.

Subjects

A total of 475 individuals were surveyed for this study. Of this total, 245 were students at Fairmont State College (FSC) and 230 were employed at a federal law enforcement agency. The respondents were chosen as a "convenience" sample, because they were easily accessible and readily available to complete the surveys. The process for survey approval at each location is discussed below.

Surveys were disseminated to 245 students in 12 social science classes at Fairmont State College in Fairmont, West Virginia. The students were enrolled in criminal justice, sociology, psychology, and history classes at various levels, including freshmen, sophomores, juniors, and seniors. Permission to survey the classes was verbally provided by the instructors for the respective classes, and the surveys were distributed to all of the students in attendance. To avoid duplication, students were instructed to only complete one survey, even if they attended more than one class that was surveyed. Students were not asked to identify their major on the survey, so the student responses were tracked by the course that they were attending when they completed the survey. The distribution of students in the classes is listed in Table 1.

Table 1

Students at Fairmont State College

	1st year student	2nd year student	3rd year student	4 or more years	Total
Criminal Justice	4	8	27	18	57
Sociology	35	18	7	5	65
History	24	29	14	10	77
Psychology	3	5	12	26	46
Totals	66	60	60	59	245

Surveys were disseminated to 290 employees of a federal agency. Prior to disseminating the surveys, approval was requested from supervisors and unit chiefs. The agency is divided into divisions, which are divided into sections, which in turn are divided into units. Unit chiefs supervise several units within a section, and supervisors are the last lines of command above the employees who were asked to complete the surveys. Two supervisors and two unit chiefs granted verbal approval for dissemination of the surveys within their respective units, for a total of four units. Written approval by a section chief was obtained for one section, which did not include the four units mentioned above, and a Deputy Assistant Director, who is a supervisor to a section chief, provided verbal approval for another separate section.

The number of surveys to disseminate was calculated based on the populations chosen. A ten percent rule was applied, as the enrollment for full and part-time students on the main campus at Fairmont State College on the Monday-Friday schedules was approximately 1,800, and a total of approximately 2,900 people were employed at the federal agency. All of the surveys distributed to FSC students were returned (100% return rate). Since the surveys were disseminated to 12 classes, three in each social science division previously mentioned, a total of 13.6% of the student population was surveyed, so that all students in a class could be included. 259 of the agency surveys were returned and an additional 29 surveys were incorrectly completed or were incomplete and could not be used. Thus, 230 surveys were usable, for a return rate of 89.31%. A total of 7.98% of agency employees were represented in the survey.

The results of the surveys were compiled into an Excel workbook, which divided the law enforcement responses, the class responses, the total student responses, and total responses to all surveys. These responses were divided into percentages, to compare between the student and agency responses. Each class section, either criminal justice, history, psychology, or sociology accounted for nearly an equal amount of the total student responses. Most of the questions received similar or the same answers from both student respondents and agency respondents. Each of these settings comprised nearly fifty percent of the total surveyed population (Fairmont State College students surveyed= 245; Law enforcement agency members surveyed= 230). The total percentages for each question from the student and agency respondents were usually very close to the same, and limited testing was conducted.

CHAPTER IV

Results

Identity Theft Awareness Survey Results

The Survey

The first section of the survey of identity theft awareness asked ten questions directly related to the subject. The first question, "Is identity theft a Federal offense?" provided three responses from which to choose. As stated in Chapter II, identity theft is criminalized in 18 U.S. Code § 1028. The next question, "Does West Virginia have a state statute addressing identity theft?" also provided three possible responses. As stated in Chapter II, West Virginia Code § 61-3-54 criminalized identity theft as a state offense. The third question asked, "Do victims usually know their perpetrators?" In only 12 percent of cases, the victims have a personal relationship with the perpetrator (FTC, 2003).

The next two questions were simply yes or no answers, with no right or wrong responses. They asked "Have you ever heard of a fraud alert?" and "Have you heard of the Federal Trade Commission?"

The last five questions of the first section provided multiple answers for selection. The first of these, "How do most criminals use the identifying information they have stolen?" Most perpetrators use the information to open new credit card accounts." The next question, "What is the most common age group of identity theft victims?" provided the same answers as the demographic information at the end of the survey. The most common age group of victims is 30-

39, although 18-29 is second and 40-49 is third. These three age groups comprise 75% of the identity theft complaints received by the FTC (FTC, 2003).

The eighth question on the survey asked, “How many credit reporting agencies are there?” and listed one through four and the option, “I did not know there were any credit reporting agencies.” There are actually three credit reporting agencies, although it provides a more accurate portrayal of awareness to state “I did not know there were any credit reporting agencies” than to guess. Question nine asked, “Who should victims call to have fraud alerts placed on their file?” The credit reporting agencies place fraud alerts on credit files. The final question of the first section asked, “What should you do if you believe your identity has been stolen?” The options were (a.) cancel all credit cards, (b.) close checking accounts, (c.) order a copy of your credit report, or (d.) all of the above. The best answer is (d.) all of the above, but in that sense, all of the above answers were correct.

The last five questions on the survey were demographic. Two of the questions, “Have you ever been a victim of identity theft?” and “Do you know someone who has been a victim of identity theft?” received responses of Yes, No, or Not that I know of. Question 13 was “Please describe your age,” which offered (a.) 18-29, (b.) 30-39, (c.) 40-49, (d.) 50-59, or (e.) 60 or over, as possible responses. The next question asked, “How were you selected to participate in this survey?” and offered the choices of (a.) I’m a student at a local college/ university, (b.) I’m employed at a federal law enforcement agency, or (c.) I’m a family member/friend of the researcher. The last question on the survey asked, “If you are a student, please identify your years in college,” and the options were (a.) 1st year, (b.) 2nd year, (c.) 3rd year, or (d.) 4 or more years.

Research Question 1

Over 70% of student and agency respondents were aware that identity theft is a Federal offense, and slightly over 16% were aware that identity theft is also a state offense. This shows that students at Fairmont State College (FSC) and members of the law enforcement agency are more aware of a Federal statute than a West Virginia State statute, as depicted in Tables 2 and 3.

Table 2

Question 1: Is identity theft a Federal offense?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Yes	186	75.92%	149	64.78%	335	70.53%	100.00 %
No	9	3.67%	23	10.00%	32	6.74	29.48%
I don't know	50	20.41%	58	25.22%	108	22.74	22.74%

Table 3

Question 2: Does West Virginia have a state statute addressing identity theft?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Yes	51	20.82%	26	11.30%	77	16.21%	100.00 %
No	37	15.10%	33	14.35%	70	14.74%	83.79%
I don't know	157	64.08%	171	74.35%	328	69.05%	69.05%

Over 75% of the students and 64% of agency respondents knew that identity theft was a Federal offense. Additionally, 20.41% of students and 25.22% of agency respondents answered, "I don't know." Nearly four percent (3.67%) of students and 10% agency respondents answered no to this first question.

In contrast, over 60% of students and nearly 75% of federal employees responded, "I don't know" to whether or not West Virginia has a state statute addressing identity theft. In student responses, more responses indicated that West Virginia does have a state statute rather than not (n=51 and n=37, respectively). In contrast, more agency responses indicated that West Virginia did not have a statute addressing identity theft than those who indicated that a statute does exist (n=33 and n=26, respectively).

A chi-square test was used to determine if there was a relationship between the responses provided by the students and agency respondents to these two questions. See Table 4 for the statistics.

Table 4

Identity theft statutes

	Federal Statute		State Statute		
	Yes	No	Yes	No	Row Sums (RS)
Student respondents					
Observed frequencies (f_o)	186	9	51	37	283
Expected frequencies (f_e)	184.4	17.6	42.4	38.5	
$(f_o-f_e)^2/f_e$	0.01	4.20	1.74	0.06	
Column percentage	55.52%	28.13%	66.23%	52.86%	
Agency respondents					
Observed frequencies (f_o)	149	23	26	33	231
Expected frequencies (f_e)	150.5	14.4	34.6	31.5	
$(f_o-f_e)^2/f_e$	0.01	5.14	2.14	0.07	
Column percentage	44.48%	71.88%	33.77%	47.14%	
Column Sums (CS)	335	32	77	70	514
Calculated X^2 statistic	13.38				
Degrees of freedom (df)	3.00				
Critical X^2 value	7.81				
Cramer's V	0.21				

Since the calculated chi-square is greater than the critical chi-square value, the research hypothesis that there is a relationship between the answers provided by the student and agency respondents is accepted. To determine the strength of this relationship, Cramer's V is applied. When interpreting the Cramer's V significance, it appears that there is a low, but definite relationship in the responses provided.

Research Question 2

Over 60% of all respondents knew that victims generally did not know their perpetrators. See Table 5 for the results to survey question 3.

Table 5

Question 3: Do victims usually know their perpetrators?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Yes	74	30.20%	41	17.83%	115	24.21%	100.00 %
No	128	52.24%	159	69.13%	287	60.42%	75.79%
I don't know	43	17.55%	30	13.04%	73	15.37%	15.37%

Over 52% of students responses reported that they believed victims did not know their perpetrators, while 30% indicated that they believed victims knew the perpetrators. Sixty-nine percent of the federal workers indicated that they believed the victims usually did not know their perpetrators, compared with 52% of the student respondents. Nearly 18% believed that victims do know their perpetrators, while 13% indicated that they did not know.

Research Question 3

Questions 4 and 9 of the survey discuss fraud alerts. As mentioned before, a fraud alert is placed on a credit account, by the credit reporting agencies, to prevent perpetrators from obtaining additional credit in the victim's name. Over 64% of all respondents had never heard of a fraud alert, as depicted in Table 6. Almost an equal amount knew that the credit reporting agencies placed fraud alerts on the accounts or stated that they did not know (34.32% and 33.68%, respectively), as shown in Table 7.

Table 6

Question 4: Have you ever heard of a "fraud alert?"

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Yes	89	36.33%	80	34.78%	169	35.58%	100.00 %
No	156	63.67%	150	65.22%	306	64.42%	64.42%

Table 7

Question 9: Who should victims call to have a fraud alert placed on their file?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
FTC	64	26.12%	40	17.39%	104	21.89%	100.00 %
Credit reporting agencies	60	24.49%	103	44.78%	163	34.32%	78.11%
Banks	13	5.31%	6	2.61%	19	4.00%	43.79%
SSA	22	8.98%	7	3.04%	29	6.11%	39.79%
I don't know	86	35.10%	74	32.17%	160	33.68%	33.68%

A majority of student respondents (63.67%) had never heard of a fraud alert and the majority of students (35.10%) did not know who to contact to have a fraud alert placed on file. This makes sense, as most individuals who have not heard of a fraud alert probably would not know who to contact to have one placed on their file.

Much like the student respondents, a majority (n=150) of agency respondents had never heard of a fraud alert. In fact, less than 35% had heard of a fraud alert. However, nearly 45 percent of agency respondents knew that a fraud alert can be placed on an account by the credit reporting agencies.

Research Question 4

Over 87% of all the respondents had heard of the Federal Trade Commission, as depicted in Table 8. The Federal Trade Commission handles more than identity theft complaints, which may be a reason that so many respondents had heard of it.

Table 8

Question 5: Have you heard of the Federal Trade Commission?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Yes	191	77.96%	225	97.83%	416	87.58%	100.00 %
No	54	22.04%	5	2.17%	59	12.42%	12.42%

In response to this survey question, 77.96% of student respondents had heard of the Federal Trade Commission. Over 97% of the federal workers had heard of the Federal Trade Commission, significantly higher than the 78% represented by the student respondents. This may be because federal employees receive more communications from the FTC than the students or because the federal respondents may be assigned to areas that share information with the FTC, but not necessarily related to identity theft.

Research Question 5

Student and agency respondents selected the same answers for survey question 6, as depicted in Table 9, and almost all of the respondents knew what to do if they believed they had been victimized, as shown in Table 10. In fact, over 70% of all respondents knew that stolen identifying information was generally used to open new credit card accounts and 21% believed that the information was used to obtain fraudulent loans, and 93% believed that victims should close checking accounts, cancel credit card accounts, and order a copy of their credit report if they believe their information has been stolen.

Table 9

Question 6: How do most criminals use the identifying information they have stolen?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Open new checking accounts	28	11.43%	3	1.30%	31	6.53%	100.00 %
Open new credit cards	145	59.18%	190	82.61%	335	70.53%	93.47%
Obtain fraudulent loans	66	26.94%	34	14.78%	100	21.05%	22.94%
Establish new telephone service	6	2.45%	3	1.30%	9	1.89%	1.89%

The majority of students, or 59.18%, knew that most criminals use the identifying information they have stolen to open new credit card accounts. Another 26.94% believed that the information was usually used to obtain fraudulent loans. Much the same, the majority of agency respondents, or 82.61%, knew that most criminals use the identifying information they have stolen to open new credit card accounts. Another 14.78% believed that the information was usually used to obtain fraudulent loans, which was the second most popular selection by agency respondents to this question.

Table 10

Question 10: What should you do if you believe your identity has been stolen?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Cancel all credit card accounts	4	1.63%	2	0.87%	6	1.26%	100.00 %
Close checking account	3	1.22%	0	0.00%	3	0.63%	98.73%
Order a copy of your credit report	8	3.27%	17	7.39%	25	5.26%	98.10%
All of the above	230	93.88%	211	91.74%	441	92.84%	92.84%

Over 93% of student respondents answered “All of the above” when asked what to do if they believed they had become a victim. The second most popular option was to order a copy of their credit report. Slightly less than 92% knew that all of the above (close credit cards, close checking account, and obtain credit report) should be done an individual believes that he or she has been a victim of identity theft. Much like the students, the second most popular answer to this question was to order a copy of a credit report.

Research Question 6

The total respondents believed that the age group most likely to be victimized is 30-39 (n=139), followed by 18-29 (n=117), and 60 and above (n=112). Table 11 shows that the student respondents and agency respondents answered this question differently. The interesting part of this was that, in many instances, the respondents' age was the same as their choice of answer for this question.

Table 11

Question 7: What is the most common age group of identity theft victims?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
18-29	89	36.33%	28	12.17%	117	24.63%	100.00 %
30-39	64	26.12%	75	32.61%	139	29.26%	75.37%
40-49	29	11.84%	49	21.30%	78	16.42%	46.11%
50-59	12	4.90%	17	7.39%	29	6.11%	29.69%
60 and over	51	20.82%	61	26.52%	112	23.58%	23.58%

Many student respondents (n=89) believed that the most common age group of identity theft victims was 18-29. While this is incorrect, it should be noted that this is the most common age group of the student respondents (n=220). Slightly over 26% knew that the most common age of identity theft victims is 30-39, while 20.82% believed that the most common age of identity theft victims was 60 and over.

Nearly 33 percent of agency respondents knew that the average age group for identity theft victims was 30-39, which coincidentally was the majority age group among the agency respondents. Over 26% believed that the most common age group of victims was 60 and over, and 21.30% believed that the most common age group of victims was between 40 and 49.

<u>Research Question 7</u>

Over 45% of all respondents knew that there were three credit reporting agencies, as depicted in Table 12.

Table 12

Question 8: How many credit reporting agencies are there?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
1	37	15.10%	17	7.39%	54	11.37%	100.00 %
2	31	12.65%	28	12.17%	59	12.42%	88.63%
3	82	33.47%	133	57.83%	215	45.26%	76.21%
4	37	15.10%	39	16.96%	76	16.00%	30.95%
I didn't know there were any credit reporting agencies	58	23.67%	13	5.65%	71	14.95%	14.95%

The majority of students (n=82) and the majority of agency respondents (n=133) had the correct answer to survey question 8. The second most popular response by the students to this question was "I did not know there were any credit reporting agencies," which received 23.67% of the responses. The second most popular response to this question by the agency respondents was four credit reporting agencies, which received 16.96% of the responses.

Research Question 8

The responses to survey questions 11 and 12, discussing personal victimization, revealed some interesting comments. While the majority responded "Yes" or "No," a small percentage of the group stated "Not that I am aware of" or "Not that I know of" to this question. This is interesting, because it implies that the survey may have sparked the respondents' interest in their own possible victimization, something that they may not have contemplated before. When combining the questions relating to whether respondents had been a victim personally or knew someone who had been a victim, nearly 800 responses indicated negative, or no. The total of 800 results from 430 student and agency respondents indicating they have not been victims, and 369 student and agency respondents indicating they did not know anyone who was a victim. Tables 13 and 14 depict the responses to these two questions.

Table 13

Question 11: Have you ever been a victim of identity theft?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Yes	10	4.08%	10	4.35%	20	4.21%	100.00 %
No	224	91.43%	206	89.57%	430	90.53%	95.79%
Not that I know of	11	4.49%	14	6.09%	25	5.26%	5.26%

Table 14

Question 12: Do you know someone who has been a victim of identity theft?

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
Yes	49	20.00%	56	24.35%	115	22.11%	100.00 %
No	195	79.59%	174	75.65%	287	77.68%	77.89%
Not that I know of	1	0.41%	0	0.00%	73	0.21%	0.21%

As expected, 91% of students indicated they had never been victimized, and only 20% indicated they knew someone who had been a victim. A total of 25% of agency respondents either had been a victim of identity theft or knew someone who was a victim. This number exceeds the national average of 20% (Survey: 1 in 5 Americans victimized by ID theft, 2003). However, this could be a biased sample, which could be more familiar with identity theft than the general population, or the victims may not all be residents of North Central West Virginia, or West Virginia at all. Additionally, some of the respondents who indicated that they knew someone who has been a victim of identity theft may have known the same person who was victimized.

Age of respondents

Within the total number of respondents, over 52% were between the ages of 18-29, as shown in Table 15. Nearly 23% were between the ages of 30-39, and 13.47% were between the ages of 40-49. This totals 88.47% of all respondents. National figures from the FTC report that 75% of reported victims of identity theft are within the same three age groups, so the sample may be seen as representative of the most likely to be victimized.

Table 15

Question 13: Please describe your age

	FSC Response	Percent of FSC	Agency Responses	Percent of Agency	Total responses	Percent of Total	Cumulative Percentage
18-29	220	89.80%	29	12.61%	249	52.42%	100.00 %
30-39	18	7.35%	91	39.57%	109	22.95%	47.57%
40-49	6	2.45%	58	25.22%	64	13.47%	24.62%
50-59	1	0.41%	46	20.00%	47	9.89%	11.15%
60 and over	0	0.00%	6	2.61%	6	1.26%	1.26%

Within the college setting, over 89% of the student respondents were between the ages of 18-29, with no student respondents falling in the 60 and over category. At the agency, nearly 40 percent were between the ages of 30 and 39, with more respondents in the 40-49 and 50-59 age groups than the 18-29 age group that dominated the student respondents.

As only students responded to question 15, regarding “years as a student,” no comparison between the student and agency responses were made. Although the classes were randomly selected within the social sciences division, the distribution among “years as a student” categories was almost even. They totaled 26.94% with one year, 24.49% with two years, 24.49% with three years, and 24.08% with four years. The responses from the four social science classes (criminal justice, sociology, history, and psychology) are depicted in Tables 16, 17, 18, and 19 in Appendix D.

Survey Comments

The last section of the survey asked for comments about the survey from the respondents. While some of the comments ranged from “Good luck” and “Interesting survey,” others included personal stories of victims and suggestions regarding public awareness. Some examples are:

“Interesting . . . I feel more should be done to raise public awareness.”

“People need to be more educated and more info needs to be given. This is a scary subject.”

“Maybe there should be some classes or sessions making people aware of this offense. I know I haven’t really heard much about it.”

“I have a checking account that I keep only for online payments…I have never lost a credit card, but I thought I did one time and I was frantic realizing how easy it would be for someone to use it.”

“A lot of questions were a little difficult to answer, having either not being a victim or not knowing of any victims.”

“I think this crime needs to be brought to everyone’s attention.”

“A person should be entitled to one free credit report a year to make sure they were not a victim of identity theft.”

“I have seen a segment on identity theft on Dateline. I know I don’t want it to happen to me.”

"I would like to see a copy of the thesis once everything is tallied…The reason I would like to see an 'update' is because I guessed at most of the questions. The only thing I really know about identity theft is what I've seen on America's Most Wanted."

"I believe the biggest chance of identity theft occurs when ordering and paying for merchandise over the Internet."

"I think the survey could start me thinking more about what seems to be becoming a serious problem and motivate me to find out the answers to these questions for my own benefit."

In reviewing these comments, it appears that the survey aroused curiosity about identity theft. While some individuals had heard about identity theft on television, others had not heard much at all and wanted to know more information. Ideas, such as offering classes or sessions about identity theft, could lead to more public awareness sessions in the communities of North Central West Virginia. Some of the comments were reflective of information in the review of the literature, such as the comment about making credit reporting agencies provide one free copy of a credit report each year, which is currently under review in Congress for new laws about identity theft.

CHAPTER V

Summary and Conclusion

Summary of Findings

Limitations

This study has several limitations. First of all, the surveys were distributed through a selection of "convenience," which means that either the researcher or an associate of the researcher knew the teachers and supervisors to authorize these surveys. Secondly, the survey did not ask where the respondents resided, so the findings cannot be generalized to the target area of North Central West Virginia. Additionally, to sample fewer than 500 people is to sample less than one percent of the population, so the received answers cannot be generalized to the target area. Finally, the survey still could be developed to be more comprehensive and ask additional questions to get a better determination of awareness in the area, such as development of a Likert scale to assess awareness regarding probability of victimization and prevention techniques.

Conclusions

Based on the findings, the conclusion can be made that many residents of North Central West Virginia are aware of the federal statute regarding identity theft, what to do if they are victimized, and that victims usually do not know their perpetrators. It could also be that the surveyed population is more informed than the general population. More information needs to be provided relative to the state statute, fraud alerts, and the credit reporting agencies. It appears that the surveyed population is slightly above the national average of 20% victimization, as 25% of the total surveyed population have been victimized or know someone who has been a victim of identity theft.

Recommendations for Further Study

This survey lends itself to enhancements and further research. A project could be completed assessing the awareness level of students on campus alone, whether at Fairmont State College, and its offsite locations, or at West Virginia University or Marshall University. This could ascertain levels of student awareness and comparisons could be made between the classes, years of education, or the schools, if more than one is selected. Surveys could also be disseminated at public meetings or other forums to get a more varied audience, or in other parts of West Virginia, or even other states and large metropolitan areas. A larger sample would be recommended if this study were reproduced. The survey itself could be enhanced to include additional identity theft information and demographic information, such as the city or county where the respondent resides, whether the respondent is male or female, if the respondent knows where most complaints of identity theft originate, and so on. Hopefully, more statistics will be available in the future that accurately portray the number of victims throughout the U.S. and in each state.

References

Biemer, J. (2002, March 18). Bills would increase penalties for identity fraud. *Associated Press Newswires*: The Associated Press.

Cohen, J. (2001, July 2). Internet insecurity. *Time*, *157*(26), 44-52.

Cullen, D. (2002, March 25). Invasion of the ID snatchers. *The Age*. John Fairfax Group Pty Ltd.

Del Grosso, R. (2001, December). How to avoid an identity crisis. *Security Management*, 45(12): American Society for Industrial Security, Arlington.

Federal Bureau of Investigation, Automated Case System (2002, June 11). *All cases for Financial Institution Fraud classification with identity theft crime problem indicator.*

Federal Trade Commission (2001, June). *Identity theft victim complaint data: Figures and trends on identity theft November 1999 through June 2001.* Retrieved April 10, 2002 from http://www.ftc.gov.

Federal Trade Commission (2001, July). *ID theft: When bad things happen to your good name*. Federal Trade Commission Headquarters: Washington, D.C.

Federal Trade Commission (2003, January 22). *National and state trends in fraud and identity theft: January – December 2002*. Federal Trade Commission Headquarters: Washington, D.C.

Flavelle, D. (2003, January 31). Company apologizes for loss of personal data; Confidential information was on hard drive. *The Toronto Star*.

Franceschina, P. (2002, June 29). Fugitive shows up in court; woman wanted in identity theft. *South Florida Sun-Sentinel*: The Sun-Sentinel.

Givens, B. (2000, July 12). *Identity theft: How it happens, its impact on victims, and legislative solutions*. Retrieved March 20, 2002 from http://www.privacyrights.org/ar/id_theft.htm

Ingram, S. (2002, May 18). Police charge South Carolina woman with identity theft. *Knight-Ridder Tribune Business News*: Newport News Daily Press.

Keefe, B. (2003, February 20). Privacy a larger issue with online resumes. *The Atlanta Journal-Constitution*.

Keeping Count with ID Theft. *Consumer Sentinel*. Volume 6, Issue 2, Summer 2001.

Lazarus, D. (2002, October 27). I found an ID thief on my credit report. *The San Francisco Chronicle*: ProQuest Information and Learning.

Lee, S. (2001, August). *Identity theft and its effect on the financial services industry*. Celent Communications: Boston, MA.

Mercury News (2002, May 31). Identity theft victim describes horrors. *San Jose Mercury News*: San Jose Mercury News.

National White Collar Crime Center {NW3C}(2001). *WCC Issue: Identity theft*. Retrieved January 15 from http://www.nw3c.org.

National White Collar Crime Center and Federal Bureau of Investigation (2001, April). *IFCC 2001 Internet Fraud Report, January 1, 2001-December 31, 2001*.

Pickler, N. (2002, March 27). Stolen identity: $30,000 in purchases, all charged to me. *Associated Press Newswires*: The Associated Press.

Rusch, J. (2001). Making a federal case of identity theft. *Consumer Sentinel, 6*(2). Federal Trade Commission Headquarters: Washington, D.C.

Stana, R. and U.S. General Accounting Office (2002, February 14). *Identity theft: Available data indicate growth in prevalence and cost*. Government Document GAO-02-424T.

Survey: 1 in 5 Americans victimized by ID theft (2003, January 20). *Credit Union Journal*. Thompson Financial Inc.

Sutherland, Edwin H. (1940). *White-collar criminality*. In Joseph E. Jacoby, *Classics in criminology* (pp. 20-25). Prospect Heights, IL: Waveland Press.

U.S. Attorney's Office, Southern District of New York (2002, November 25). *U.S. announces what is believed the largest identity theft case in American history; losses are in the millions.* U.S. Department of Justice Press Release.

U.S. Census Bureau (2003). Geographic Comparison Table for West Virginia Counties. Retrieved March 22, 2003 from http://factfinder.census.gov.

U.S. General Accounting Office {US GAO}(1998, May). *Identity fraud: Information on prevalence, cost, and Internet impact is limited*. Government Document GAO/GGD-98-100BR.

U.S. General Accounting Office {US GAO} (2002, March). *Identity theft: Prevalence and cost appear to be growing*. Government Document GAO-02-363.

Watts, R. (2002, March 31). Banks pass the buck on fraud. *Sunday Telegraph London*: The Telegraph Group Limited.

West Virginia Legislature (n.d.). West Virginia Code §61-3-54. Retrieved March 22, 2003 from http://www.legis.state.wv.us/scripts

Appendix A

A SURVEY OF IDENTITY THEFT AWARENESS

You are asked to complete the following survey regarding your awareness of identity theft and the laws protecting the victims. Please answer all questions completely and to the best of your knowledge. Your answers will be kept confidential and consolidated with all other returned surveys for an assessment of identity theft awareness.

PART I: PERSONAL EXPERIENCE

Have you or anyone close to you been a victim of identity theft? If so, please document the circumstances as you remember, including how you identified the theft, what steps you took to report the theft, and how you felt at the time. Also include your interaction with law enforcement, specifying the levels, and how you felt through the process. Finally, please discuss what steps you took to correct your credit and how much time this took, as well as cooperation in the financial industry.

PART II: IDENTITY THEFT KNOWLEDGE

The following questions are to be answered with a "Yes" or "No," or by circling the best answer.

1. Is identity theft a Federal offense?

2. Do states have laws addressing identity theft?

3. How do most criminals use the identifying information they have stolen:

   a. Open new checking accounts
   b. Open new credit card accounts
   c. Obtain fraudulent loans
   d. Establish new telephone service

4. What is the most common age group of identity theft victims:
   a. 18-29
   b. 30-39
   c. 40-49
   d. 50-59

e. 60 and over

5. Which city reports the highest number of complaints:
   a. Miami
   b. Chicago
   c. New York City
   d. Los Angeles

6. Do most victims know their perpetrators personally?

7. How many credit bureaus are there:
   a. 1
   b. 2
   c. 3
   d. 4
   e. I did not know there were any credit bureaus

8. Have you ever heard of a "fraud alert?"

9. Who should be contacted immediately if you believe your identity has been stolen:
   a. Creditors
   b. Local police
   c. Credit reporting agencies
   d. FBI

10. Have you ever heard of the Federal Trade Commission?

Appendix B

IDENTITY THEFT AWARENESS SURVEY

Please circle the best answer--PLEASE CIRCLE ONLY ONE--to the following questions.

1. Is identity theft a Federal offense?
    a. Yes
    b. No
    c. I don't know

2. Does West Virginia have a state statute addressing identity theft?
    a. Yes
    b. No
    c. I don't know

3. Do victims usually know their perpetrators?
    a. Yes
    b. No
    c. I don't know

4. Have you ever heard of a "fraud alert"?
    a. Yes
    b. No

5. Have you heard of the Federal Trade Commission?
    a. Yes
    b. No

6. How do most criminals use the identifying information they have stolen:
    a. Open new checking accounts
    b. Open new credit card accounts
    c. Obtain fraudulent loans
    d. Establish new telephone service

7. What is the most common age group of identity theft victims:
    a. 18-29
    b. 30-39
    c. 40-49
    d. 50-59
    e. 60 and over

8. How many credit reporting agencies are there:
    a. 1
    b. 2
    c. 3

d. 4
e. I did not know there were any credit reporting agencies

9. Who should victims call to have a fraud alert placed on their file:
   a. Federal Trade Commission
   b. Credit reporting agencies
   c. Banks
   d. Social Security Administration
   e. I don't know

10. What should you do if you believe your identity has been stolen:
    a. Cancel all credit card accounts
    b. Close checking account
    c. Order a copy of your credit report
    d. All of the above

Personal Questions: Please answer for demographic purposes in this study

11. Have you ever been a victim of identity theft?

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

13. Please describe your age:
    a. 18-29
    b. 30-39
    c. 40-49
    d. 50-59
    e. 60 or over

14. How were you selected to participate in this survey:
    a. I'm a student at a local college/university
    b. I'm employed at a federal law enforcement agency
    c. I am a family member/friend of the researcher

15. If you are a student, please identify your years in college:
    a. 1st year
    b. 2nd year
    c. 3rd year
    d. 4 or more years

If you have any comments regarding this survey, please list them here:

Appendix C

MARSHALL UNIVERSITY™
www.marshall.edu

Office of Research Integrity
Institutional Review Board

MEMORANDUM

To: **Gwendolyn Lea Goodrich**
Criminal Justice
MUGC

From: **Henry K. Driscoll, M.D.**
Marshall University IRB #1 Chairperson HD

Date: **March 12, 2003**

Re: **IRB Exempt Study No. EX03-0062 – Identity Theft Awareness in North Central West Virginia**

Thank you for the submission of the above anonymous survey study. The purpose of the study is to assess how familiar people are with identity theft.

The study as submitted would be exempt from IRB review and approval in accordance with 45 CFR 46.101 b. Please submit a progress report of the study prior to March 12, 2004 or <u>upon completion and/or closure</u> of the study if prior to the anniversary date.

HKD/tjs

EX03-0062goodwichmarch12-03

401 11th Street, Suite 1300 • Huntington, West Virginia 25701 • Tel 304/696-7320
A State University of West Virginia • An Affirmative Action/Equal Opportunity Employer

Appendix D

Responses to Fairmont State College surveys by discipline

Table 16

Students surveyed in criminal justice courses

Question 1: Is identity theft a Federal offense?		
a. Yes	48	84.21%
b. No	1	1.75%
c. I don't know	8	14.04%
Question 2: Does West Virginia have a state statute addressing identity theft?		
a. Yes	15	26.32%
b. No	12	21.05%
c. I don't know	30	52.63%
Question 3: Do victims usually know their perpetrators?		
a. Yes	16	28.07%
b. No	36	63.16%
c. I don't know	5	8.77%
Question 4: Have you ever heard of a "fraud alert"?		
a. Yes	30	52.63%
b. No	27	47.37%

Question 5: Have you heard of the Federal Trade Commission?

a. Yes	46	80.70%
b. No	11	19.30%

Question 6: How do most criminals use the identifying information they have stolen:

a. Open new checking accounts	2	3.51%
b. Open new credit card accounts	38	66.67%
c. Obtain fraudulent loans	16	28.07%
d. Establish new telephone service	1	1.75%

Question 7: What is the most common age group of identity theft victims:

a. 18-29	17	29.82%
b. 30-39	15	26.32%
c. 40-49	6	10.53%
d. 50-59	4	7.02%
e. 60 and over	15	26.32%

Question 8: How many credit reporting agencies are there:

a. 1	10	17.54%
b. 2	6	10.53%
c. 3	28	49.12%

d. 4	6	10.53%
e. I did not know there were any credit reporting agencies	7	12.28%

Question 9: Who should victims call to have a fraud alert placed on their file:

a. Federal Trade Commission	15	26.32%
b. Credit reporting agencies	17	29.82%
c. Banks	5	8.77%
d. Social Security Administration	4	7.02%
e. I don't know	16	28.07%

Question 10: What should you do if you believe your identity has been stolen:

a. Cancel all credit card accounts	1	1.75%
b. Close checking account	0	0.00%
c. Order a copy of your credit report	5	8.77%
d. All of the above	51	89.47%

Question 11: Have you ever been a victim of identity theft?

Yes	4	7.02%
No	51	89.47%
Not that I know of	2	3.51%

Question 12: Do you know someone who has been a victim of identity theft?

Yes	17	29.82%
No	39	68.42%
Not that I know of	1	1.75%

Question 13: Please describe your age:

a. 18-29	52	91.23%
b. 30-39	2	3.51%
c. 40-49	3	5.26%
d. 50-59	0	0.00%
e. 60 and over	0	0.00%

Question 15: If you are a student, please identify your years in college:

a. 1st year	4	7.02%
b. 2nd year	8	14.04%
c. 3rd year	27	47.37%
d. 4 or more years	18	31.58%
	57	
Percent of FSC	23.27%	

Table 17

Students surveyed in sociology courses

Question 1: Is identity theft a Federal offense?		
a. Yes	46	70.77%
b. No	4	6.15%
c. I don't know	15	23.08%
Question 2: Does West Virginia have a state statute addressing identity theft?		
a. Yes	11	16.92%
b. No	8	12.31%
c. I don't know	46	70.77%
Question 3: Do victims usually know their perpetrators?		
a. Yes	18	27.69%
b. No	36	55.38%
c. I don't know	11	16.92%
Question 4: Have you ever heard of a "fraud alert"?		
a. Yes	26	40.00%
b. No	39	60.00%

Question 5: Have you heard of the Federal Trade Commission?

a. Yes	52	80.00%
b. No	13	20.00%

Question 6: How do most criminals use the identifying information they have stolen:

a. Open new checking accounts	9	13.85%
b. Open new credit card accounts	37	56.92%
c. Obtain fraudulent loans	17	26.15%
d. Establish new telephone service	2	3.08%

Question 7: What is the most common age group of identity theft victims:

a. 18-29	18	27.69%
b. 30-39	23	35.38%
c. 40-49	10	15.38%
d. 50-59	3	4.62%
e. 60 and over	11	16.92%

Question 8: How many credit reporting agencies are there:

a. 1	13	20.00%
b. 2	11	16.92%
c. 3	17	26.15%

d. 4	10	15.38%
e. I did not know there were any credit reporting agencies	14	21.54%

Question 9: Who should victims call to have a fraud alert placed on their file:

a. Federal Trade Commission	15	23.08%
b. Credit reporting agencies	21	32.31%
c. Banks	5	7.69%
d. Social Security Administration	10	15.38%
e. I don't know	14	21.54%

Question 10: What should you do if you believe your identity has been stolen:

a. Cancel all credit card accounts	2	3.08%
b. Close checking account	1	1.54%
c. Order a copy of your credit report	1	1.54%
d. All of the above	61	93.85%

Question 11: Have you ever been a victim of identity theft?

Yes	4	6.15%
No	59	90.77%
Not that I know of	2	3.08%

Question 12: Do you know someone who has been a victim of identity theft?

Yes	11	16.92%
No	54	83.08%

Question 13: Please describe your age:

a. 18-29	56	86.15%
b. 30-39	7	10.77%
c. 40-49	2	3.08%
d. 50-59	0	0.00%
e. 60 and over	0	0.00%

Question 15: If you are a student, please identify your years in college:

a. 1st year	35	53.85%
b. 2nd year	18	27.69%
c. 3rd year	7	10.77%
d. 4 or more years	5	7.69%
	65	
Percent of FSC	26.53%	

Table 18

Students surveyed in history courses

Question 1: Is identity theft a Federal offense?		
a. Yes	60	77.92%
b. No	3	3.90%
c. I don't know	14	18.18%
Question 2: Does West Virginia have a state statute addressing identity theft?		
a. Yes	19	24.68%
b. No	10	12.99%
c. I don't know	48	62.34%
Question 3: Do victims usually know their perpetrators?		
a. Yes	23	29.87%
b. No	36	46.75%
c. I don't know	18	23.38%
Question 4: Have you ever heard of a "fraud alert"?		
a. Yes	25	32.47%
b. No	52	67.53%

Question 5: Have you heard of the Federal Trade Commission?

a. Yes	56	72.73%
b. No	21	27.27%

Question 6: How do most criminals use the identifying information they have stolen:

a. Open new checking accounts	15	19.48%
b. Open new credit card accounts	41	53.25%
c. Obtain fraudulent loans	19	24.68%
d. Establish new telephone service	2	2.60%

Question 7: What is the most common age group of identity theft victims:

a. 18-29	32	41.56%
b. 30-39	18	23.38%
c. 40-49	9	11.69%
d. 50-59	4	5.19%
e. 60 and over	14	18.18%

Question 8: How many credit reporting agencies are there:

a. 1	10	12.99%
b. 2	9	11.69%
c. 3	21	27.27%

d. 4	15	19.48%
e. I did not know there were any credit reporting agencies	22	28.57%

Question 9: Who should victims call to have a fraud alert placed on their file:

a. Federal Trade Commission	21	27.27%
b. Credit reporting agencies	15	19.48%
c. Banks	2	2.60%
d. Social Security Administration	6	7.79%
e. I don't know	33	42.86%

Question 10: What should you do if you believe your identity has been stolen:

a. Cancel all credit card accounts	1	1.30%
b. Close checking account	2	2.60%
c. Order a copy of your credit report	1	1.30%
d. All of the above	73	94.81%

Question 11: Have you ever been a victim of identity theft?

Yes	1	1.30%
No	71	92.21%
Not that I know of	5	6.49%

Question 12: Do you know someone who has been a victim of identity theft?

Yes	15	19.48%
No	62	80.52%

Question 13: Please describe your age:

a. 18-29	73	94.81%
b. 30-39	4	5.19%
c. 40-49	0	0.00%
d. 50-59	0	0.00%
e. 60 and over	0	0.00%

Question 15: If you are a student, please identify your years in college:

a. 1st year	24	31.17%
b. 2nd year	29	37.66%
c. 3rd year	14	18.18%
d. 4 or more years	10	12.99%
	77	
Percent of FSC	31.43%	

Table 19

Students surveyed in psychology courses

Question 1: Is identity theft a Federal offense?		
a. Yes	32	71.11%
b. No	1	2.22%
c. I don't know	13	28.89%
Question 2: Does West Virginia have a state statute addressing identity theft?		
a. Yes	6	13.33%
b. No	7	15.56%
c. I don't know	33	73.33%
Question 3: Do victims usually know their perpetrators?		
a. Yes	17	37.78%
b. No	20	44.44%
c. I don't know	9	20.00%
Question 4: Have you ever heard of a "fraud alert"?		
a. Yes	8	17.78%
b. No	38	84.44%

Question 5: Have you heard of the Federal Trade Commission?

a. Yes	37	82.22%
b. No	9	20.00%

Question 6: How do most criminals use the identifying information they have stolen:

a. Open new checking accounts	2	4.44%
b. Open new credit card accounts	29	64.44%
c. Obtain fraudulent loans	14	31.11%
d. Establish new telephone service	1	2.22%

Question 7: What is the most common age group of identity theft victims:

a. 18-29	22	48.89%
b. 30-39	8	17.78%
c. 40-49	4	8.89%
d. 50-59	1	2.22%
e. 60 and over	11	24.44%

Question 8: How many credit reporting agencies are there:

a. 1	4	8.89%
b. 2	5	11.11%
c. 3	16	35.56%

d. 4	6	13.33%
e. I did not know there were any credit reporting agencies	15	33.33%

Question 9: Who should victims call to have a fraud alert placed on their file:

a. Federal Trade Commission	13	28.89%
b. Credit reporting agencies	7	15.56%
c. Banks	1	2.22%
d. Social Security Administration	2	4.44%
e. I don't know	23	51.11%

Question 10: What should you do if you believe your identity has been stolen:

a. Cancel all credit card accounts	0	0.00%
b. Close checking account	0	0.00%
c. Order a copy of your credit report	1	2.22%
d. All of the above	45	97.78%

Question 11: Have you ever been a victim of identity theft?

Yes	1	2.22%
No	43	95.56%
Not that I know of	2	4.44%

Question 12: Do you know someone who has been a victim of identity theft?

Yes	6	13.33%
No	40	88.89%

Question 13: Please describe your age:

a. 18-29	39	86.67%
b. 30-39	5	11.11%
c. 40-49	1	2.22%
d. 50-59	1	2.22%
e. 60 and over	0	0.00%

Question 15: If you are a student, please identify your years in college:

a. 1st year	3	6.67%
b. 2nd year	5	11.11%
c. 3rd year	12	26.67%
d. 4 or more years	26	57.78%
	46	
Percent of FSC	18.78%	

Curriculum Vitae

Gwendolyn Lea Goodrich

407 State Street

Fairmont, WV 26554

Education:

Bachelor of Arts Degree, Major in History; Double Minor in French and Criminal Justice, obtained from Fairmont State College, May 1996.

Master of Science Degree, Criminal Justice, obtained from Marshall University, May 2003.

Work Experience:

Disk jockey, WRLF/WTCS, Fairmont, WV	August 1991-October 1992
Cashier, Community Foodland, Fairmont, WV	September 1992-April 1995
Federal Government	April 1995-Present
Typist	April 1995-July 1995
Fingerprint Examiner	July 1995-June 2000
Intelligence Research Specialist	June 2000-Present