

**“IDENTITY THEFT”
ASSISTING VICTIMS IN THEIR RECOVERY**

E.M.U. SCHOOL OF POLICE STAFF AND COMMAND

**Sergeant Kevin P. Murphy
Flat Rock Police Department**

**An applied research project submitted to the Department of Interdisciplinary
Technology as part of the School of Police Staff and Command Program
September 19, 2003**

ABSTRACT

Identity theft is the fastest growing crime in the country. The Flat Rock Police Department has had little experience in handling identity theft fraud cases but has seen an increase over the last three years. What is identity theft and how does it affect the citizens of Flat Rock? How do you investigate crimes that occur outside your jurisdiction and what can the police do to assist ID theft victims? The researcher used a descriptive method of research to answer these questions. He gathered most of his material from the Internet for it held a vast amount of information which was current. Newspaper articles were reviewed to gather insight on how victims are impacted. The researcher also reviewed the FRPD's case files for 2001, 2002, and 2003 to determine the extent of the problem in Flat Rock.

The researcher found that the epidemic of identity theft affects 10 million people and costs the U.S. economy billions of dollars each year. This epidemic will only get worse before it gets better. There are a variety of methods used by ID thieves to steal one's personal information from the low tech method of "Dumpster Diving" to the high tech method of hacking into large databases. The consumer, law enforcement, and the business community must become equal partners in stemming the tide of identity theft.

The consumer can reduce the risk of ID theft by becoming more vigilant in protecting their personal information. Law enforcement must educate themselves in order to educate and protect their citizens. The business community, especially banks and credit card companies, need to invest in technology that encrypts and protects databases and authenticates and verifies users.

The researcher recommends that the Flat Rock Police Department take the initiative to educate its officers so that they can protect its citizens.

TABLE OF CONTENTS

ABSTRACT.....	2
TABLE OF CONTENTS.....	3
INTRODUCTION	4
BACKGROUND AND SIGNIFICANCE.....	5
LITERATURE REVIEW	18
PROCEDURES.....	19
RESULTS	20
DISCUSSION	20
RECOMMENDATIONS.....	21
REFERENCE LIST	22
APPENDIX A.....	24

INTRODUCTION

Identity theft is the fastest growing crime in the United States that has caught the attention of the media in the last few years. The victims are faced with years of financial ruin and emotional stress as they try to recover their identity. Law enforcement has been slow to address this new criminal trend for several reasons. Indifference to the effects identity theft has on the victims, ignorance to the methods criminals use, the lack of technical skills and resources, and the question of jurisdiction have often hampered law enforcement's ability to assist victims in their recovery.

The researcher observed that the Flat Rock Police Department has seen an increase in reported identity theft cases. The researcher set out to see how identity theft had impacted the citizens of Flat Rock and how effective the police department was in investigating the crime and assisting the victim.

The researcher found that the department had received a small number of identity theft cases and that the financial toll had been minimal. However, the department had been ineffective in resolving these cases and little assistance was given to the victim after the initial report.

What were the problems facing the department and what resources and skills were needed to improve the investigation and resolution of these cases? How can the Flat Rock Police Department educate its citizens in preventing identity theft? How can law enforcement assist victims in their recovery? The researcher's goal was to answer these questions and develop plans and procedures to improve customer service.

The researcher used a descriptive method to research identity theft. He reviewed three years of reported identity theft cases from the Flat Rock Police Department to gain insight into the problems the department was facing. The Internet was extensively utilized for resource material. Newspapers were perused for the extent of frustration crime victims face.

BACKGROUND AND SIGNIFICANCE

Identity theft experts previously thought that an estimated 500,000 to 700,000 Americans were victims of identity theft each year and that millions of dollars were lost each year (FTC). A new survey of 4,000 adults conducted for the Federal Trade Commission shows that the fastest growing crime in this country has exploded to affect 10 million people with an estimated loss of billions of dollars (Dugas). A victim of identity theft can expect months and sometimes years of frustration and anguish as they attempt to pick up the pieces of their decimated financial history and recover their identity. The devastating effects of identity theft have moved the International Association of Chiefs of Police to pass two resolutions. One calls for the legislative branch of state governments to enact laws that create and/or increase penalties for criminals who steal another person's identity (IACP). The other resolution calls for law enforcement to take a more active role in taking and investigating cases of identity theft and to refer victims to the FTC's hotline at 1-877-IDTHEFT and to the Identity Theft Clearinghouse (IACP).

Technology has improved the lives of millions of Americans but it has also made it easier for savvy criminals to gather personal information that is stored in databases and use that information to victimize unsuspecting citizens. The Internet has provided the white collar criminal with an effective means to prey on today's society. Computers are used extensively in modern business and most are vulnerable to outside intrusion of their databases. An

accomplished ID thief can steal a person's personal information, create a new identity, establish credit, purchase items online, direct delivery to a commercial mailbox, and arrange for these packages to be delivered by courier without leaving his computer desk and little risk of apprehension. Meanwhile, it takes months before the victim becomes aware that there is a problem. Credit cards statements and phone calls from bill collectors are often the first clues that identity theft has occurred.

The victim naturally contacted their local police department and until recently was told, "Contact your credit card company," (IACP) and left without a report being taken or a report was taken for 'Informational Purposes Only' and little or no effort was taken to investigate the matter. Victims were further frustrated when they contacted their credit card company and were told that since they were not a party to the fraudulent account, they were not entitled to the company's database for the company had to protect the imposter's privacy rights (ITRC). "Banks are often reluctant to acknowledge that they have an identity theft problem and find it more cost effective to write the loss off rather than report it. The bank then passes the cost along to the consumer through higher interest rates according to Christine Pratt, a senior analyst in TowerGroup's consumer credit practice" (Hawkins). "Beth Givens, director of the Privacy Rights Clearinghouse thinks that passing the buck to the consumer is unfair and that lenders would immediately change their ways of authenticating identity and verifying information if they had to pay for the collateral damage identity theft causes" (Hawkins).

Stealing Your Identity

Personal information is used daily to conduct business. People need to use their personal information to write checks, use their credit cards, buy alcohol, visit the doctor, pay bills, and borrow library books. This information is stored in computer databases, paper documents,

credit card receipts, and utility bills. Large databases like the Department of Motor Vehicles and small ones like the local video rental stores are fertile hunting grounds for predators to victimize unsuspecting prey. Thieves have both low tech and high tech ways of gathering personal information.

A person's Social Security number [SSN] is the Holy Grail for the identity thief. That 9 digit number is designated to identify a person from cradle to grave and is used nationwide as a personal identifier. A thief can obtain a driver's license, establish credit, open bank accounts, obtain employment, and file for bankruptcy using a stolen Social Security number. Social Security numbers are vulnerable to abuse but are widely used and stored in today's business practices. Health insurance companies use and print the number on their subscriber's insurance cards. Some states' Department of Motor Vehicles print the SSN as well as the Driver's License number on the Driver's License. Colleges and the military use the Social Security number to identify their students and employees.

An identity thief can steal personal information in a variety of ways. "Dumpster Diving" (USDOJ) is the practice of sifting through people's garbage to obtain information. Discarded utility bills, credit card receipts, healthcare statement, prescribed medication bottles and instructions, and pre-approved credit card application provide a wealth of information that the thief can manipulate to his advantage. "Shoulder Surfers"(USDOJ) hang out near the ATM machine, the cash register, and public pay phones, and peek over an unsuspecting person's shoulder to view or hear when that person punches in his PIN or calling card number or recites his address, phone number, or SSN for the cashier. "Insider trading" can occur when an authorized person accesses a database and uses that information for illegal means. The thief may use that information for himself or may sell the information to identity theft rings. Identity

thieves may also bribe or pay unscrupulous cashiers or attendants for copies of credit card transactions. Computer savvy “Crackers” (Hitchcock) may hack into large databases and download personal information. Identity thieves can also use the Internet to legally obtain personal information. “The U.S. Securities and Exchange Commission [SEC] stopped requiring that people stop using their SSN even though there was a space on their online form. The online version of the *Congressional Record* has a policy of announcing all promotions of military officers holding the rank of colonel or higher. Included in the announcement was the officer’s military ID number which is their SSN. They have since partially redacted a portion of the SSN but the full number still appears in the original print version” (Hitchcock p.103).

Identity thieves may also call a person at home and impersonate a bank official and request that the person verify their personal information. The thief may have done some homework and provide the victim with the home address and vehicle make in an attempt to authenticate their status as an official. The victim will volunteer the information and become suspicious only after they hang up the phone and the damage is done.

“Thieves can also steal purses and wallets from persons, vehicles, and the workplace. Outgoing mail can be stolen and personal checks used to pay bills can be submerged in chemicals which remove the ink but leave the check unblemished. Pre-ordered checkbooks can be stolen from the mailbox or at the mail distribution center. The information from these checks can be used to order duplicate checks through the Internet and allow the thief to take over the account” (Pollock and May).

Your mail can also be diverted to another location when an identity thief completes a “change of address form” at the local post office. They may also fraudulently obtain your credit report by posing as a landlord or employer (FTC).

Cashing In

Stolen personal information can be used in a variety of ways to enrich the criminal. The most common method is through credit card fraud. A thief may obtain a new credit account, a duplicate card, or use a stolen credit card to make large purchases before the card is reported missing and the account is closed. They may call the credit card company and request a change of address so that the billing statements are diverted to another location. This extends the card's usefulness to the thief.

Checking accounts can be opened and bad checks can be written in the victim's name. The counterfeit checks can drain a person's account and cause the victim to accumulate fees and penalties when the checks are returned for Non-Sufficient Funds [NSF] or closed accounts. The thief may then file for bankruptcy in the victim's name to avoid detection.

The thief may use stolen information to receive a valid Driver's License or Social Security card. The thief then is free to rack up points for traffic violations and commit crimes in the victim's name. They can skip out on court appearances resulting in criminal bench warrants being issued in the victim's name.

Phone services are the most abused utility services by identity thieves. Thieves can 'clone' your cellular phone or open a landline account in your name. They may steal and use your calling card and PIN to make long-distance phone calls.

Thieves can use your Social Security number to file a fraudulent tax return or to commit investment fraud. Thieves have also used stolen identity to obtain healthcare and commit welfare fraud.

Preventing Identity Theft

Identity theft is seen as an unstoppable and unavoidable crime. However, the consumer, the business community, and law enforcement can take action to prevent and reduce identity theft. Private citizens can reduce the risk of becoming victims of identity thieves by educating themselves on how identity thefts occur. The Internet can provide a wealth of information and resources in helping to prevent theft and recover from it should it occur. The Federal Trade Commission is the lead agency in the fight against identity theft. They operate a website, www.ftc.gov, which provides the consumer with information about identity theft. They have developed a pamphlet titled *ID Theft: When Bad Things Happen to Your Good Name* which offers these tips on prevention:

- Order a copy of your credit report from each of the three major reporting agencies every year. View it for accuracy and authorized activities. The three major credit bureaus are: Equifax at www.equifax.com, Experian at www.experian.com, and TransUnion at www.transunion.com. The companies are allowed to charge up to \$9.00 per copy but the U.S. House of Representatives have recently passed a bill that would allow citizens to receive a free copy of their credit report each year upon request (Holland).
- Place passwords on your credit card, bank and phone accounts. Passwords should not contain easily available information and should be at least eight digits long with numbers and letters and at least one symbol.
- Secure personal information at home especially if you have roommates or expect strangers to enter the home to provide service.
- Ask your employer how personal information is stored and who has access to that information. Postings for the public should not contain your full name. Find out how documents with your personal information are disposed.

- Don't give out personal information over the phone, through the mail, or over the Internet unless you're the one who had initiated contact. Thieves may pose as bank representatives, ISP providers, or government employees in an attempt to scam personal information. Many companies post scam alerts on their websites when their names are used fraudulently.
- Deposit outgoing mail in post office collection boxes or at the local post office. Remove incoming mail immediately and have the post office hold the mail if you are on vacation.
- Thwart the efforts of "Dumpster Divers" by using a criss-cross shredder on all documents that may contain personal information. Be sure to include all those pre-approved credit applications.
- Find out why and how personal information is to be used before filling out any applications or conducting any business transactions.
- Don't carry your Social Security number card in your wallet or purse. Leave it at home in a secured area.
- Carry only the identification cards and credit cards that you actually use.
- Pay attention to your billing cycles and contact your creditors if they bills do not arrive on time.
- Be aware of promotional scams especially in the form of e-mail spam.
- Keep your purse or wallet in a safe place at work. Do not leave it exposed in your vehicle. A locked vehicle offers little resistance to a determined thief.

The U.S. Department of Justice, www.usdoj.gov, has provided these additional measures that can be taken to make it more difficult for identity thieves:

- Use a gel pen when writing checks. The ink can not be removed by chemicals.

- Survey the immediate area before conducting business at the ATM machine or public telephone.
- Request that your name be removed from telemarketer's databases.
- Maintain careful records of your banking and financial accounts.
- Adopt a "Need to Know" approach to your personal information. Be stingy and refuse to offer your vital information just because a cashier or application asks for it.

The Federal Trade Commission also recommends that people 'harden' their personal computers by following these tips:

- Update virus protection software regularly, or when a new virus alert is announced. Crackers can introduce destructive codes into your computer causing it to send out files.
- Do not open e-mails from unknown sources or download files sent to you by strangers. Do not click on hyperlinks from people you don't know.
- Use a firewall program, especially if you are connected to a high-speed internet connection like DSL, cable, or a T-1 line. These systems allow your computer to be connected to the Internet 24 hours a day. They also allow a cracker to remotely access your files when you are away from the computer. Log off of the computer when not in use to add a layer of security should your firewall fail.
- Use a secure browser that has the most up-to-date encryption security when conducting business online.
- Try not to store financial information on your laptop computer. Use a strong password if you do. Do not use the automatic log-on feature and log off each

time you are through with the laptop. Do not store your laptop in an exposed place.

- Be sure to remove personal information before disposing of the computer. Either physically destroy the hard drive or utilize a “wipe” utility program that stacks random code until the information is beneath too many layers to be retrievable.

For more information on clearing your hard drive go to:

www.hq.nasa.gov/office/oig/hq/harddrive.pdf

- Look for website privacy policies. They answer how your information is stored. If you don't see a privacy policy, consider another site.

The FBI's Internet Fraud Complaint Center, www.ifccfbi.gov, offers these suggestions when bidding at Internet auctions:

- There should be no reason to give the seller your Social Security number or Driver's license number.
- Make sure your transaction is secure before you electronically send your credit card numbers.
- Consider using an escrow or alternate payment service. This allows you to pay indirectly through a reputable middleman thus avoiding direct payment to an unfamiliar seller.

Most criminals avoid challenges and seek opportunities. Private citizens may not be able to totally eliminate the risk of identity theft but they can reduce the criminal's opportunities through education and vigilance.

Law Enforcement's Role in ID Theft Prevention

In general, law enforcement has been slow in responding to the serious of identity theft. Ignorance and indifference have hampered effective investigations and have caused added frustration for the victim. The first step a chief can take in battling identity theft is educating his patrol officers and detectives. Professional, well intentioned officers are seen as indifferent when taking identity theft cases because they may be ignorant on how identity theft works and frustrated that they can not immediately identify and arrest a suspect. Law enforcement may not be able to immediately act on identity theft cases but they can become more active in informing the public and acting as advocates for victims.

Matthew Lease and Tod Burke presented some strategies in an article for the *FBI Law Enforcement Bulletin* on how police can prevent ID Theft. They are:

- Patrol residential areas on trash collection days and during tax season.
- Enforce trespass laws with regard to residential and commercial dump sites.
- Advise citizens to shred documents and drop off mail in a locked mailbox.
- Remind people to be cautious when using ATMs and public phones.
- Disseminate information to the public on how to reduce and prevent computer, credit, and cellular phone fraud.
- Suggest restrictions to businesses to reduce internal access fraud.
- Educate officers on methods of identity theft and the resulting types of fraud.

Police departments engaged in community policing can be very effective in preventing identity theft. The community contacts have already been established and the networks are already in place. Police departments that have not adopted the community policing concept can also be very effective. These departments can get the message out through several methods:

- Prepare an article for the city's newsletter or local newspaper. Most local newspapers relish the opportunity to partner with the local police department in providing information that benefits the public.
- Prepare a pamphlet and distribute to local businesses, libraries, and churches. The contacts made through distribution allow the department an opportunity to receive feedback and gauge the severity of ID Theft in their community.
- Organize seminars for prospective college students and their parents to inform them on ways to protect their identity on campus and in their dorm rooms.
- Post messages on your department's website or local access cable channel. Small packages of information can be effective in generating interest. Be prepared to follow up with more comprehensive material.
- Contact local civic groups and request to make a presentation. Most civic organizations enjoy a visit from their police department.
- Set up an information booth at the city's annual event.
- Provide pamphlets at the front desk of police department.
- Encourage officers to find opportunities to inform the public in groups or one-on-one when taking calls.

Law enforcement is encouraged to develop alliances with the local business community, the banking industry, and the major credit card companies. Local police departments can develop relationships with their business community to find out what kinds of problems the businesses may be having and offer strategies that businesses could use to help the police prevent and investigate fraud.

The FTC has also established two databases to assist investigators of identity theft. The Identity Theft Data Clearinghouse lists over 300,000 cases to help locate similar cases, victims, and suspects. The FTC's Consumer Sentinel allows investigators to see reported cases in their area so that trends, additional victims, or suspects could be identified (FTC).

The Business Community's Responsibility

The consumer, law enforcement, and the business community must become equal partners to stem the tide of identity theft. Retailers and lenders need to realize that the problem will get worse before it improves. Bob Berardi, a Los Angeles Deputy Sheriff assigned to Identity Theft Task Force, states that the banking industry needs to be more cooperative for they tend to withhold bogus credit card applications. "It's easier to keep it quiet, write it off, and go," says Berardi (Hawkins).

Christine Pratt from TowerGroup stated, "Until lenders suffer even more substantial losses, they can't justify the expenditures necessary to verify identity (Hawkins). Beth Givens, director of the Privacy Rights Clearinghouse, blames the explosion of identity theft on the lending industry. "They make it too easy to get credit and do not do a good enough job examining credit applications (Dugas).

The Federal Trade Commission recently released a statement that identity theft cost American consumers and businesses 53 billion dollars in 2002 (Holland). Retailers and lenders can reduce this staggering figure by investing in technology and changing business practices.

Retailers and credit card companies could require that a PIN be used for all transactions. All debit cards and some credit cards that allow cash advances already have PINs to authenticate the user. PINs could also be required for personal checks.

Biometric authentication is an emerging technology that can aid the business industry in reducing fraud. An individual's unique physical characteristics, [fingerprints, voice, eyes, faces, and written signature], can be captured in electronic format. This electronic data could be imbedded in credit, debit, or ATM cards and be used to authenticate the user at point-of-sale transactions (Pollock and May).

Lenders can also reduce identity theft by verifying the information on applications and investigate irregularities such as misspelled names, address, and omission of information.

Retailers can require photo identification and obtain thumbprints when accepting credit cards and personal checks.

Recovering from Identity Theft

Victims of identity theft can expect to face months and years of frustration once they fall prey to predatory identity thieves. bill collectors, bank officials, and government employees can further exacerbate the situation. The Federal Trade Commission, the Identity Theft Resource Center, and The Privacy Rights Clearinghouse are just a few agencies dedicated to helping ID Theft victims. These identity theft experts suggest several ways to help a person recover their identity. The FTC's guide, *ID Theft: When Bad Things Happen To Your Good Name*, suggests that the first three things a person should do are:

- Contact the fraud departments of each of the three credit bureaus. Tell them you're a victim of identity theft and request that a fraud alert be placed in your file. Also request a statement requesting that lenders call you before opening new accounts.
- Close the accounts you know or suspect to be tampered with or open fraudulently.
- File a report with your local police department and in the community where the theft or fraud took place. Provide as much documentation as you can. Be persistent in your request for a

police report. Advise the officer that a report is needed to clear your name. Obtain a copy of the finished report, not just a case number.

Identity theft victims are encouraged to organize their case and keep a journal of all activity. They should write down the date, time, name of person contacted, and a summary of all conversations. They should make copies of all document sent or received. Victims should contact the FTC and file a report. The FTC also has an ID Theft Affidavit that can be filled out and is accepted by all major credit card companies and the three major credit bureaus (FTC).

LITERATURE REVIEW

The researcher was able to extensively use the Internet for resource material. Technology must be utilized as a tool in the fight against identity theft. The Federal Trade Commission and other agencies dedicated to stopping identity theft operate websites that provide helpful tips for victims attempting to recover their identities. The FTC's guide *ID Theft: When Bad Things Happen to Your Good Name* is a comprehensive guide that outlines how ID thieves operate. It provides useful information to help prevent identity theft and to assist victims in their recovery.

The Identity Theft Resource Center posts several articles on its websites that offers tips for victims and law enforcement on how to collaborate to effectively investigate identity theft. The researcher found these articles to be very informative and pertinent as they explained how victims should approach law enforcement and how law enforcement can assist the victim. The idea of accepting the victim as a "limited partner" was intriguing. The victim can aid the investigator by collecting documents and making phone calls while the investigator can maintain control and prevent the victim from acting in ways that might jeopardize the case. The researcher learned that a major complaint of ID theft victims was the lack of cooperation from

law enforcement. This perception of indifference was properly identified as not a lack of professionalism but a lack of understanding and ability to immediately help the victims. The research conducted allowed the researcher to gain a firm grasp on the problems facing victims and the ability to direct victims to the resources available to them. The Internet also provided the researcher with the most recent findings on ID Theft. The initial research material from the FTC quantified the number of victims in the hundreds of thousands and the financial loss in the millions. The FTC recently announced the results of a survey that put the number of victim's at 10 million and the financial loss in the billions. The fast growing pace and use of sophisticated techniques should be a wake up calls for local police department to develop strategies and partnerships for fight this epidemic.

PROCEDURES

The researcher used the descriptive method for his research due to his lack of knowledge of identity theft. He gathered most of his resource materials from the Internet and perused the local newspapers for articles relating to identity theft. The Internet sources provided most of the factual material while the newspaper articles provided insight into the frustration victims feel. The researcher also analyzed the last three years worth of identity theft/fraud cases that the Flat Rock Police Department had taken [See Appendix]. He observed that the problem has been relatively small but the department had been ineffective in investigating these cases and little or no support had been offered to the victims. The researcher was able to determine that the Flat Rock Police Department could better serve their citizens and become more effective in investigating identity fraud through proper training of its road officers and detectives.

RESULTS

Identity theft is the fastest growing crime in this country. It affects millions of people and costs billions to the U.S. economy. The citizens of Flat Rock have not yet been severely impacted by identity theft but the police department has seen an increase in complaints of ID theft/fraud. The department lacks the resources to properly investigate these cases but could become more effective through proper training. This training could include awareness instruction for the road officers and the detectives investigating the cases could be informed of the resources and networks that have been established to aid in the investigation and prosecution.

DISCUSSION

The researcher, like most Americans, was aware that identity theft was a problem, but was surprised at how pervasive it had become in modern society. The statistics had dramatically changed from the beginning of the project to the culmination. The researcher gained a better understanding of the problems victims must overcome in the recovery of their names. The local police departments have been a source of frustration for victims because most departments have not prepared their road officers to assist victims. The question of jurisdiction and lack of an identifiable suspect have impeded effective investigations of these cases. The reluctance of the police to get involved has given the victims the perception that the police do not care. Victims come to the police station for information and guidance but find out that their police department are just as or more ignorant of the problem if identity theft.

RECOMMENDATIONS

The researcher recommends that the Flat Rock Police Department invest the time and expense in preparing their officers to provide quality service to their citizens when investigating identity theft fraud. The road officers who are tasked in taking the taking the initial report should be trained in how identity theft occurs, how it impacts victims, how to prevent it, and ways to recover from it. The department should explore ways to educate and remind their citizens about identity theft prevention. They can use the city's newsletter and Web page to disseminate information. A resource pamphlet should be developed and distributed to the local businesses, churches, and civic groups. A recovery packet should be assembled for distribution to ID theft victims so that they are better prepared for their long journey in recovering their name. The road officers should be encouraged in finding opportunities to inform citizens on prevention techniques.

The detective bureau should be encouraged to develop contacts and alliances within the local business community and the major credit card fraud departments. The department should sign up for access to the Sentinel and other providers of information on identity theft.

The Flat Rock Police Department can improve the services they provide by progressively confronting identity theft. Their professional image can be improved through stronger relationships with the local businesses and civic groups. The victim's perception of indifference on the part of the police department can be eliminated through education and implementation of these recommendations.

REFERENCE LIST

- Dugas, C. (2003, September 4). Federal survey: Identity theft hits 1 in 4 U.S. households. *USA TODAY*, p.10B
- Federal Trade Commission. *Testimony on Identity Theft*. Retrieved April 17, 2003, from <http://www.ftc.gov/opa/2002/02/idtestimony.htm>
- Federal Trade Commission. *ID Theft: When Bad Things Happen To Your Good Name*. Retrieved April 17, 2003, from <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm>
- Hawkins, D. (2003, May 19). Hide and they can't seek. *U.S. News & World Report*, 134, 17, p. 39.
- Holland, J. J. (2003, September 11). Identity theft bill gets OK. *Detroit Free Press*, p. A2
- Identity Theft Resource Center. *Criminal Identity Theft: What to Do if It Happens to You*. Retrieved June 27, 2003, from <http://idtheftcenter.org/html/fs111.htm>
- International Association of Chiefs of Police. *Resolutions: Federal and State Legislation*. Retrieved July 17, 2003, from http://www.theiacp.org/Resolutions/index.cfm?fusaction=dis_public_view&resolution_id...

International Association of Chiefs of Police. *Resolutions: Technology and*

Curbing Identity Theft. Retrieved July 17, 2003, from

http://www.theiacp.org/Resolutions/index.cfm?fusaction=dis_public_view&resolution_id...

Internet Fraud Complaint Center. *Internet Fraud Prevention Measures*. Retrieved

August 13, 2003, from <http://www.ifccfbi.gov/strategy/fraudtips.asp>

Lease, M., & Burke, T. (2000, Aug). Identity Theft A Fast-growing Crime

[Electronic version]. *FBI Law Enforcement Bulletin*, 69 pp. 8-13.

Pollock, J., & May, J. (2002, June). Authentication Technology [Electronic

version]. *FBI Law Enforcement Bulletin*, 71, pp.1-4.

United States Department of Justice. *Identity Theft and Fraud*. Retrieved June 27,

2003, from <http://usdoj.gov/criminal/fraud/idtheft.html>

APPENDIX A

Flat Rock Police Department		
Identity Theft Case Summary		
Year	Type	Financial Loss
2003	Utility Fraud/phone	\$532.00
	Credit Card Fraud/Internet	274.00
	Utility Fraud/phone	698.00
	Credit Card Fraud	475.00
	Credit Card Fraud	4,500.00
	Impersonation	0
	Driver's License Fraud	0
	Library Fines	53.00
	Credit Card Fraud	100.00
	Credit Card Fraud	849.00
Total	10	\$7481.00
2002	Utility Fraud/phone	\$1,200.00
	Debit Card Fraud	310.00
	Credit Card Fraud	160.00
	Driver's License Fraud	0
	Credit Card Fraud attempt	0
	Utility Fraud/phone	516.00
	Credit Card Fraud	*
Total	7	\$2186.00
2001	Credit Card Fraud	\$201.00
	Credit Card Fraud	529.00
	Credit Card Fraud	200.00
	Credit Card Fraud	1,300.00
	Credit Card Fraud	38.00
	Credit Card Fraud	573.00
	Credit Card Fraud	*
Total	7	\$2841.00