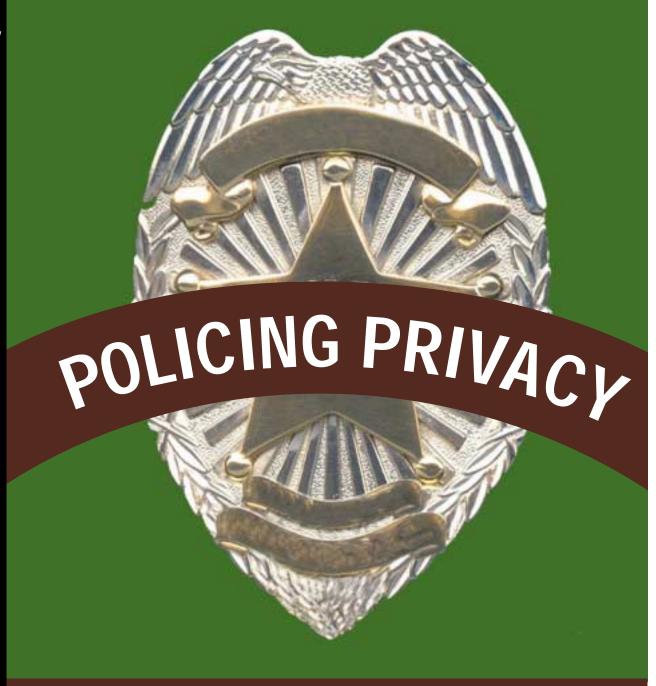
February 2004



Michigan Law Enforcement Officers On The Challenges Of Tackling Identity Theft

PIRGIM

Policing Privacy

Michigan Law Enforcement Officers
On the Challenges of Tackling Identity Theft

Megan Owens

PIRGIM

February 2004

Acknowledgements

PIRGIM gratefully acknowledges Jay Reynolds, Retail Liaison Officer for the Troy Police Department for providing thoughtful review of the report.

PIRGIM would also like to thank all of the law enforcement officers who generously shared their knowledge and experience for the writing of this report (full list in Appendix 2).

In addition, PIRGIM would like to thank Jasmine Vasavada for editing assistance and Jane Wong for the cover design.

The author alone bears responsibility for any factual errors or misquotes.

© 2004 PIRGIM

For additional copies of this report, send \$10 (including shipping) to:

PIRGIM 122 S. Main Street, Suite 370 Ann Arbor, MI 48104

The Public Interest Research Group in Michigan (PIRGIM) is a non-profit, non-partisan organization working throughout Michigan to preserve the environment, protect consumers and promote democracy. For more information about PIRGIM, please call 734-662-6597 or visit www.pirgim.org.

Table of Contents

Executive Summary	4
Background	5
Key Findings	6
Survey Finding #1 – Identity theft is on the rise	6
Survey Finding #2 – Identity theft offers unique challenges to investigators	6
Survey Finding #3 – Identity theft occurs in a variety of ways	8
Table 1 – Top methods to steal identities	8
Table 2 – Top ways identities are exploited	9
Summary of Officers' Recommendations	12
Policy Recommendations	12
Recommendations for Consumers	13
Recommendations for Companies	15
Conclusion	16
Appendix 1 – Interview Questions	17
Appendix 2 – Law Enforcement Officers Interviewed	18

Executive Summary

Identity theft is the fastest-growing crime in the country, with reported cases of identity theft nearly doubling every year.

This report summarizes interviews PIRGIM held with Michigan law enforcement officers from September 2003. These officers are on the front lines of the efforts to slow the identity theft crime wave. Their unique and often unheard perspective results from their contact with every aspect of the crime, as well as the multiple players involved – the victims, the credit lenders, the thieves and the prosecutors.

From their observations and conclusions, we hope to shed light on policies that can help prevent identity theft in the future.

The key findings from PIRGIM's survey are:

1. Identity theft is on the rise.

Every officer who responded to the question of whether the frequency of identity theft cases had changed over the past five years agreed that it had increased. 47% of officers claimed to have witnessed a significant or tremendous increase.

2. Identity theft poses unique challenges to law enforcement officers.

Law officers reported that very few identity theft cases are solved, because of the anonymity of the crime, jurisdictional challenges, lax security measures by many companies and lack of cooperation by many companies.

3. Most law enforcement officers feel new policies would help deter identity theft.

Several recommendations were offered for new laws or policies to either stop identity theft from occurring or make identity thieves easier to track and prosecute:

- Require credit card companies and other credit grantors to tighten security before granting credit;
- Ensure lenders and other companies cooperate with police investigations;
- Strengthen privacy laws to prohibit companies from selling customers personal information.

Criminalizing identity theft is not enough. Despite Congressional action to criminalize identity theft in 1998, with the state of Michigan following suit in 2000, identity theft complaints continue to grow.

These findings may provide additional guidance to policymakers seeking to provide new legal and administrative tools to those whose job it is to tackle this rapidly growing crime.

Background

Identity theft is the fastest growing crime in America, according to both the Federal Bureau of Investigations and the Federal Trade Commission. Every 79 seconds an identity is stolen. Annual fraud losses are estimated to be in excess of \$12 billion worldwide.

Each year, more and more people are grappling with the harrowing and frustrating experience of having their identity stolen. Identity theft is the unauthorized use of another's personal identifying information, such as a social security number or credit card number, to obtain credit, goods, services, medical records or employment, or to commit an illegal act. It can be as straightforward as using someone else's credit card number for a purchase or as in depth as getting a job or even getting arrested under a false identity.

Numerous reports and surveys have helped to shed light on the experiences of identity theft victims. These victims of consumer fraud must deal with unhelpful credit bureaus and collection agencies as they attempt to restore their credit history. Often complicating their efforts to clear their names is the lack of conclusive evidence that fraud has occurred. Yet all too often, even in the face of significant evidence, the criminal who committed the identity theft is never brought to justice.

With this report, PIRGIM has sought to capture the unique perspective of law enforcement officers.

Investigating identity theft is a daunting task. In an ordinary theft case, the police can check for fingerprints or go door to door to talk to potential witnesses. In an identity theft case, the traditional police methods no longer apply. When a detective receives a case, the victim will often have no idea who the thief was or how the thief gained access to his or her identity. After filing a report, the detective will seek information from the central processing houses of the banks that lent credit to the thief (usually in a different state). Although the officer will explain that the credit file includes fraudulent information and is needed for the investigation, the lending institution often refuses to share this information without a search warrant. Even with a search warrant, the bank sometimes refuses to cooperate if it is issued from a state different from the one in which its headquarters are located.

The detective is out of luck.

And so is the victim.

Identity theft has exposed archaic rules and a system that was developed to deal with old fashioned and straightforward theft. It has left detectives and investigators grappling with the hassles of tracking down an identity thief. This survey probes these hassles and starts to rethink the archaic system that essentially encourages identity thieves to continue to commit their crimes.

Key Findings

As the individuals who deal with the crime of identity theft from the moment they take down a victim's report to the time they testify in court, law enforcement officers have a unique and important perspective of the crime that can help inform efforts by citizens and policymakers to create additional barriers to identity theft.

PIRGIM held initial interviews with 22 law enforcement officials across Michigan, as well as ten in-depth interviews with the officers who investigate identity theft cases. They reported from their personal experience on the front lines of identity theft crime. While officers were quick to point out that there is no single type of identity theft case and therefore no single way to investigate identity theft crime, several key findings emerged from the survey.

Some findings simply confirmed trends that have been documented in numerous studies – for example, the finding that every officer has noted an increase in identity theft cases over the past five years.

Other findings were more surprising to those outside of the law enforcement community – for example, the finding that one of the most common types of identity theft in Michigan is to open utility service (phone, electric, cable) in someone else's name.

These findings confirm that there are many steps that we as a society can take to slow the rising trend of identity theft.

Survey finding #1: Identity theft is on the rise

"Identity theft calls have roughly doubled in my three years as a detective."
- Farmington Hills Detective Larry Fetherolf

All officers were asked whether they perceived an increase in the number of identity theft complaints their department had received over the past five years. All of the officers who responded to that question reported an increase.

While 11% reported just a slight increase, 47% of officers reported a significant or tremendous increase. Several reported that cases have doubled during that time.

Survey finding #2: Identity theft offers unique challenges to investigators

"I've been on the bureau for 26 years – identity theft cases are definitely more challenging than most other cases."

- Port Huron Detective Lieutenant Herb Welser

When asked how many of their identity theft cases were solved, officers reported that very few of their cases were solved. While many officers were unable to give a numeric estimate, several

estimated that 10% or fewer cases were solved.

Several reasons were offered for why identity theft cases are particularly difficult. Reasons cited most often included the anonymity of the crime, lax security by companies, stolen information often used outside the jurisdiction of the victim, and lack of cooperation by companies in responding to law enforcement inquiries (which in turn makes prosecution difficult).

Anonymity

"The main problem is simply identifying a suspect – identity theft is too anonymous a crime."

- Dearborn Detective Sergeant Craig Lankford

The biggest challenge is the anonymity of the crime of identity theft. The very crime of claiming a false identity means that officers usually do not have a suspect on which to start their investigation. Unlike traditional thefts, in identity theft cases there are frequently no fingerprints or witnesses. Without a name or a lead, officers report that it is very difficult to backtrack and find a suspect. Additionally, thieves often switch identities frequently and avoid leaving a paper trail. Several officers reported that the best chance of catching an identity thief occurs when they use the identity in person and are caught on video or leave fingerprints.

Companies not focused on security

"Too often people bend or ignore the rules for the sake of convenience or customer service – that allows the criminals to act. Convenience makes us very sloppy."

— Troy Retail Liaison Officer Jay Reynolds

Several officers commented that many companies feel that any efforts to increase security would hurt customer service and could hurt sales. In an effort to make purchases and financial transactions simple for customers, many companies make identity theft simple for criminals. Credit card companies were especially singled out for this problem. Credit cards are easily opened with just a name and a social security number, with little or no identity verification. Credit card companies make such a large profit off of new credit card accounts that they prefer to write off identity theft losses as a cost of doing business rather than prevent identity theft by strengthening identity verification efforts.

Lack of cooperation by companies involved

"One of the biggest problems is dealing with the credit card companies and banks – they won't give us the information we need (copies of checks and falsified applications), they really don't care about the losses."

- Farmington Hills Detective Larry Fetherolf

Another significant challenge in solving identity theft cases is companies who are unwilling to give evidence to investigators. Credit card companies often refuse to give a law enforcement officer a copy of a falsified credit application without receiving a warrant, and may not accept a

warrant from a different state. Similarly telephone companies often refuse to give information without a subpoena and will often charge the law enforcement officials for searching for the information. They claim concern over liability, but end up stalling criminal investigations.

Jurisdictional challenges

"All too often, information stolen from someone here is used in multiple places, often far away. I'm working on a case right now in Hawaii."

- Livingston County Detective Robert Michaels

Additional challenges occur because of the location of the crime. Unlike physical crimes, the thief is often not in the same city or even the same state as the victim. Most identity theft is done over the phone or internet. Crimes can occur in multiple places which makes investigations much more difficult. Some detectives are limited to tracking cases specifically within their city or county. Even when an investigator is able to track down a thief, getting witnesses to come to trial from out of state is a challenge.

Legal structure that fails to acknowledge consumers as victims

"The problem is that by law it's the companies who are the victims, and it's hard to get them to cooperate."

- Port Huron Detective Lieutenant Herb Welser

In the eyes of the law, the victim is the company who bore the financial loss, not the consumer whose identity was stolen. Companies are willing to absorb the cost of the theft and add it into their cost of doing business. They are unwilling to track and prosecute a relatively small dollar loss. Without a proven financial loss, the consumer victim is often unable to prosecute.

Survey finding #3 – Identity theft occurs in a variety of ways

Officers were asked the most common ways personal identifying information is stolen and most common ways stolen identities are used. The officers noted a variety of ways, listed in Table 1.

Table 1 –

Top Methods Used to Steal Identities

Stolen purses and wallets

Dumpster Diving

Stolen Mail

Insecure Internet Information

Relative, coworker or employee

According to the officers, most people do not know how their identity was stolen. Some of the most common ways thieves use to steal the information needed to steal identities are as follows:

Stealing purses or wallets

"With a stolen wallet or purse, an identity thief can open a checking account in someone else's name and write a ton of checks – easily spending \$5,000 in one weekend."

- Grand Rapids financial crimes detective Mark Groen

Most people's purses and wallets provide a variety of ways to steal an identity. In addition to credit card numbers that thieves can use to make unauthorized charges, many wallets contain social security numbers as well. Although most people know not to carry their social security card, many health care, student and other identification cards contain social security numbers. With a name, address, date of birth, driver's license number and social security number, an identity thief has everything he or she needs to steal an identity.

Dumpster diving

"One common way information is stolen is through dumpster diving – looking through someone's trash to find personal information."

- Livingston County Detective Robert Michaels

Most people's trash also contains the information an identity thief needs, including credit card number and bank account numbers, in addition to name, address and social security number.

Stealing mail

"Mail solicitations are a big problem – a thief can just pick a credit card application or advance check out of a mailbox."

- Dearborn Detective Sergeant Craig Lankford

Thieves also gather identity information from stealing mail. In addition to bank and credit card statements, mail often includes credit card solicitations and unsolicited convenience checks. Thieves can easily cash a convenience check or fill out pre-approved credit card applications with a different address to open a credit card in someone else's name. In addition, a book of checks stolen from the mail is a goldmine for an identity thief.

Internet

"We will eventually need to regulate the internet in order to fight crime. Just like we need traffic laws to keep the roads safe, we need regulations to keep the internet safe."

- Troy Retail Liaison officer Jay Reynolds

A great deal of personal information is available on the internet, some legally, more through illegal but widely available means.

Relative, coworker or employee

"One major point of data compromise is in getting a mortgage or refinancing a home—the application includes every possible piece of personal information, and that data goes through too many hands without nearly enough security."

- Southfield Detective Dennis Paryaski

During normal transactions, such as purchasing a house, applying for a job, opening a new back account or leasing a car, a great deal of personal identifying information is required. This information often goes through many different hands - some honest, others less honest. One common way personal identifying information is stolen is by a dishonest employee who has access to this type of information. The thief can either use the information themselves or sell it to other criminals to use.

Additionally, there have been numerous cases in which an identity thief will steal a family member's identity by forging their name on checks or other documents.

Identities can be stolen in a variety of ways, as listed in Table 2. The most common uses of personal information for identity theft include:

Table 2 –
Top Ways Identities are Exploited
Utilities Accounts
Cell Phone Accounts
Credit Card Accounts
Mail Orders
Internet Purchases

Utilities

"All too often a phone company or electric utility will give out phone or electric service with only a name and social security number. Then two years later a collection agency is chasing an innocent person."

- Saginaw Detective Bob Ruth

Almost unanimously, law enforcement officers identified one of the most common types of identity theft to be opening utility or phone service in another person's name. Most electric, gas, cable, and telephone companies give out service with only a name and social security number, with little or no verification of identity. Property owners or leasers are not held liable; investigators have to prove who specifically set up the service to prosecute, which is nearly impossible. Unpaid bills can pile up for many months before service is shut off and the victim whose information was used is suddenly faced with enormous bills they were completely unaware of.

Cellular phones

"Getting cell phone service is the most common way identity theft occurs – thieves get several cell phones charge onto someone else's credit card and burn them out, spending something thousands of dollars in calls before the phones are cut off."

- Farmington Hills Detective Larry Fetherolf

Setting up cellular phone service with someone else's credit card is also one of the top forms of identity theft. Also, cellular phone service is frequently taken directly from a checking account, allowing an identity thief to charge the bill to someone else. Criminals involved in other types of crime will use cell phones in someone else's name not only to avoid paying their bill, but also to keep their illegal activities from being tracked.

Credit cards

"We need to rein in the credit card companies – they've got to tighten security if we're ever going to stop identity theft."

- Dearborn Detective Sergeant Craig Lankford

In addition to making charges with someone else's credit card number or getting an additional card sent to a different address, thieves often open up a new credit card in someone else's name. Credit card companies make such a profit off of each card that they are primarily focused on getting cards out to customers, not confirming that the person opening the card is who they say they are. All too often a credit card is granted with only the name and social security number matching – with the address, date of birth and other information wrong.

Purchases over the phone or internet

"With so much done over the phone or internet, so anonymously, identity theft is hard to stop. We are victims of our own technology."

- Southfield Detective Dennis Paryaski

One common way identity theft occurs is for a thief to order products through a catalogue or on the internet and have it delivered to a different address. Telephone and internet commerce makes it very easy for identity theft to occur, with little or no verification of identity when purchases are made.

Summary of Officers' Recommendations

Officers' made recommendation on various ways to slow identity theft, including recommendations for law or policy changes, recommendations for consumers and recommendations for companies.

One recurring recommendation was the need for more resources. Many officers noted that while they could spend all of their time working on identity theft cases, they also work on many other cases as well. Others said they would like to have another officer working on identity theft in addition to themselves. Several noted that they often only had time to take a police report and give the victim suggestions on how to clear their record, and not enough time to thoroughly research the case and track down the thief.

Policy Recommendations

The following are PIRGIM-supported recommendations that were suggested independently by several officers interviewed as ways to either stop identity theft from occurring or make it easier for law enforcement officers to track and prosecute the identity thieves.

Policy Recommendation #1 – Require credit card companies and other credit grantors to verify the identity of a new customer before granting credit.

"I wish that companies wouldn't be so greedy. They need to be more careful in checking people out before giving out credit."

- Saginaw Detective Bob Ruth

The excessive faulty lending of credit needs to be curtailed. Credit grantors should be required to do more in-depth background checks to be sure applicants are who they say they are, and stop relying on social security numbers as the sole or primary form of identification. Too frequently, credit is granted based on a matching name and social security number, but at a different address with an incorrect date of birth. At least four identity points should match before credit is granted.

Policy Recommendation #2 – Require companies to give investigators evidence.

"One of the biggest challenges in addressing identity theft cases is getting companies to cooperate. Banks, credit unions, even the post office – they're trying to protect their clients, but the client is actually the crook."

Saginaw Detective Bob Ruth

In order to enable law enforcement officials to do their job tracking down identity thieves, companies should be required to give investigators copies of falsified applications, checks and other evidence in a timely manner. Too often, companies require a subpoena or warrant before giving law enforcement officers or victims evidence.

Policy Recommendation #3 – Prohibit companies from selling consumers personal information without their affirmative consent.

"There should be privacy laws that prohibit companies from selling customers' personal information."

- Dearborn Detective Sergeant Craig Lankford

Identity theft will never be stopped as long as large amounts of personal information are broadly available. Companies should not be permitted to trade or sell personal information. Companies should be required to receive affirmative "opt-in" permission from consumers before doing so. Private information should be kept private, owned by the consumer.

Other policy recommendations offered by officers included:

- Technological fixes such as pin numbers on credit cards or the use of biometric information like thumbprints;
- Increased penalties and mandatory jail time;
- Banning of pre-approved credit card offers;
- Holding property owners or leasers responsible for illegal utility service; and
- Regulation of the Internet.

Recommendations for Consumers

Several officers noted that even the most careful consumer cannot completely protect him or herself from all identity theft crimes. However, officers did make several recommendations for consumers wanting to decrease their chances of being a victim of identity theft:

Consumer recommendation #1 – Avoid giving out social security numbers

"I always recommend that people don't carry their social security card with them and only give out your social security number when absolutely necessary. Often you can use another ID if you ask."

- Port Huron Detective Lieutenant Herb Welser

Nearly all officers interviewed strongly voiced the need to not give out personal information unless absolutely necessary, especially social security numbers. When asked for a social security number, consumers should ask if they can use an alternate number or form of identification. Do not carry your social security number in your wallet unless necessary. Do not print your social security number on checks.

Consumer recommendation #2 – Shred documents containing personal information

"Everyone concerned about identity theft should buy a shredder, to make sure no one can steal your information from your trash."

- Mark Groen, Grand Rapids financial crimes detective

Many officers strongly recommended purchasing a shredder and shredding all personal documents, including bank statements, credit card receipts and pre-approved credit card offers, before throwing them out.

Consumer recommendation #3 – Check your credit report regularly

"Everyone should check their credit report at least once a year."

- Mark Groen, Grand Rapids financial crimes detective

Officers suggested that everyone should order a copy of their credit report regularly, to both look for errors (which are common) and to spot potential identity theft problems early. Identity theft victims should check their credit reports every few months to ensure the problem hasn't restarted.

Consumer recommendation #4 – Watch your credit card statement carefully

"Always watch your credit card bills carefully and report any discrepancies immediately."

- Detroit Lt. James Elliot

Know when your credit card statement arrives each month and read it carefully. Immediately report to your credit card company if your statement does not arrive when expected or if you notice any discrepancies on you statement.

Consumer caution – There is no way to completely stop identity theft

"Unfortunately no one is immune from identity theft. As long as your personal information is out there in lots of hands, identity theft is going to continue to happen."

- Southfield Detective Dennis Paryaski

The unfortunate caution offered by most officers interviewed is that although there are many steps that can be taken to decrease your chance of being a victim of identity theft, there is no way to completely protect yourself. There is a great deal of private information publicly available, companies continue to be lax in verifying identities and identity theft is profitable enough that it will continue to occur despite a consumers best efforts. That does not mean that consumers or companies have an excuse to be sloppy or lazy in their security practices, but it is the unfortunate reality.

Recommendations to Companies

Banks, retailers and other companies have an important role to play in stopping identity theft. Officers offered several recommendations to companies who want to protect their customers and employees from identity theft.

Company recommendation #1 – Verify customers' identities carefully

"Some banks or stores try to be so customer friendly that they allow fraud to happen."

- Troy Retail Liaison Officer Jay Reynolds

Law enforcement officers strongly urge companies to be vigilant in confirming customers' identities. Require customers to have identification, check it carefully. Teach employees to be cautious. Many identity thieves have been caught by a careful salesperson noticing something that doesn't seem right.

Company recommendation #2 – Shred old records

"Companies should always be careful with records and shred all records before disposing of them."

- Port Huron Detective Lieutenant Herb Welser

Identity thieves can find a gold mine when companies throw out old financial records without shredding them. Companies should always shred documents when getting rid of customer or employee records.

Company recommendation #3 – Don't use social security numbers except for tax purposes

"In order to protect both employees and customers, companies should avoid using social security numbers, especially on pay sheets."

- Livingston County Detective Robert Michaels

Companies should not use social security numbers as identification numbers on identification cards or pay sheets. Although employers must use social security number on tax documents, companies should protect their employees by not using them for any other purposes.

Conclusion

Clearly identity theft is a large and growing problem, both in Michigan and nationally. Law enforcement officers are working hard to address this problem, but face unique challenges that make their job difficult. In order to protect the people of Michigan from the crime of identity theft, Michigan laws need to be updated and law enforcement officers need to be given more tools and resources. Hopefully policy makers, consumers and companies will heed the recommendations offered by these experts in identity theft law.

Appendix 1 - Interview questions

Preliminary interviews

The interview process began with brief initial interviews of police from a wide range of cities and counties, including both the cities with the most reported cases of identity theft and smaller cities and counties. These interviews were conducted in August of 2003.

Hi, my name ..., work with the Public Interest Research Group in Michigan. We're doing research on the problem of identity theft - surveying police departments across the state. I've got a few questions that I'd like to ask to you or someone in the department. It should take just 2-3 minutes.

- How many identity theft calls would you estimate that your office receives in an average month?
 - o Has that changed over the past five years? How?
- Who do identity theft cases go to?
 - What portion of their time is spent on identity theft?
 - o Have they received training on identity theft specifically?
- How many people work in your police/sheriff department? (note officers or full staff)
- What is your name, title/position?

In-depth interviews

The second half of the interview process was to follow up with police officers who worked specifically on identity theft and ask them a longer set of questions. These interviews were done in September of 2003.

Hi, my name is . . . , work with the Public Interest Research Group in Michigan. I believe you spoke with someone from my office a few weeks ago regarding our research into the problem of identity theft in Michigan. I'd like to ask you a few follow-up questions. Do you have 5-10 minutes now or is there a better time for me to call?

- [Confirm who identity theft calls go to and approximately how much time is spent on identity theft]
 - o Approximately how many get solved in a given month?
 - O When a case is solved, how much time would you estimate it takes?
- In your experience, what are the most common ways identity theft occurs?
- Are there unique challenges to addressing identity theft cases?
 - o What are the biggest challenges in dealing with identity theft cases?
 - o How could these challenges be minimized?
 - What would be the one law or policy change you think would make the biggest difference in stopping or solving identity theft?
 - o Any other law or policy changes you feel would be useful?
- What advice do you give to people to protect themselves from identity theft?
- What can companies do to protect their customers from identity theft?
- Anything else I should know?
- [confirm title and spelling of name]
- How long have you been on police force? How long have you been in your current position?
- [confirm how many people on police staff]

Thank you

Appendix 2 – Police interviewed

Initial interviews

Bay City - Char Thayer, Records Clerk

Berrien County dispatcher

Cheboygan County dispatcher

Chippewa County - Detective Carry

Dearborn - Detective Sergeant Lankford

Detroit - Lieutenant James Elliot

Farmington Hills - Detective Fetheroff

Grand Rapids - Captain Hertel, commander of investigations

Houghton County - Roy Britz

Lansing - Lieutenant Bruce Ferguson

Lapeer County - Lieutenant Parks

Livingston County - Lieutenant Rob Michels

Macomb County - Sergeant Sheldon

Mt. Pleasant - Detective Sergeant Bloomer

Muskegon - Captain John Workman, captain of detective bureau

Port Huron - Detective Lieutenant Herb Wellser

Royal Oak - Lieutenant Don Foster, in charge of detective bureau

Saginaw - Detective Ruth

Southfield - Detective Dennis Paryaski

Traverse City - Deputy Newingham

Troy - Retail Liaison Officer Jay Reynolds

Warren dispatcher

Note – We attempted to reach other rural counties, but do not have a county sheriff department, instead relying on the state police.

In-depth interviews:

- 1) Detective Lieutenant Herb Welser, Port Huron Police Department Interviewed 9/2/03
- 2) Detective Larry Fetherolf, Farmington Hills Police Department Interviewed 9/8/03
- 3) Lieutenant James Elliot, Detroit Police Department Interviewed 9/8/03
- 4) Detective Lieutenant Robert Michaels, Livingston County Police Department Interviewed 9/8/03
- 5) Detective Sergeant Craig Lankford, Dearborn Police Department Interviewed 9/8/03
- 6) Lieutenant Don Foster, Lt in charge of detective bureau, Royal Oak Police Department

Interviewed 9/17/03

- 7) Detective Mark Groen, Grand Rapids Police Department Interviewed 9/17/03
- 8) Detective Bob Ruth, Saginaw Police Department Interviewed 9/17/03
- 9) Retail Liaison Officer Jay Reynolds, Troy Police Department Interviewed 9/17/03
- 10) Detective Dennis Paryaski, Southfield Police Department Interviewed 9/22/02