STATEMENT
OF
DONALD REBOVICH

Executive Director, Center for Identity Management
And Information Protection
Utica College

Information Policy, Census, and National Archives Subcommittee
Oversight and Government Reform Committee
Wednesday, June 17, 2009
2154 Rayburn HOB
2:00 p.m.

Chairman Clay, Ranking Member McHenry and Distinguished Members of the Subcommittee:

Good afternoon, Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to appear before you to discuss the serious crime of identity theft, the impact that it has on its victims and what can be learned from criminological research in these areas.

As with any emerging crime area, the acknowledgment of identity theft as a distinct brand of criminality largely rests with the popularly accepted perception of the act itself as being, in some way, threatening to the average person. In general, the individual forms his or her own opinion about an emerging crime area based upon a combination of published reports of examples of notorious case incidents, broadcast vignettes depicting the unfortunate experiences of the victims, media announcements cautioning against behavior that may precipitate victimization, and, quite often, simple word-of-mouth. The frequency and the veracity of the conveyance of this type of information become powerful driving forces in the manner in which the general public synthesizes the information and draws conclusions about the actual level of danger the crime poses to them. Sometimes referred to as the *commonsense methodology*, this thought process is not the methodology of science outlined in textbooks on logic, but is impressionistic, highlighting general tendencies rather than specific interpretations.

Such has been the case with the quest to understand identity theft. While no less than a decade ago, the term was apt to be met with curiosity and some bewilderment, it has become one of the most recognizable emerging crime terms in the 21st century. But, while the term may be familiar to many, questions still remain regarding what the term really represents, what type of person is most likely to commit this crime, what criminal methods are most commonly (and successfully) employed, and who is in the most jeopardy of being victimized. To strengthen our abilities to genuinely contain and prevent identity theft, these questions must be answered not through a speculative commonsense methodology, but through an *empirical* approach anchored in a thorough analysis of criminal justice system data.

The greatest challenge that the instinctive public acceptance of a speculative commonsense assessment of identity theft characteristics presents to the law enforcement community is that it can misleadingly color the characterization of identity theft by the very officials responsible for controlling it. The subjective view of what is represented by the term "identity theft" can prove to be deceptively contagious as it bleeds over from the general populace to enforcement circles at the local, state and federal levels. A substitution of one's own subjective biases and experience for an empirical approach, has led to the ruin of many misguided law enforcement programs and initiatives. As expressed by noted criminologists, like Brown and Curtis, many practitioners within the criminal justice system have met with repeated failure because they relied upon only their common sense. Thus, millions of dollars have been spent on police patrol efforts that do not reduce crime, judicial practices that are widely perceived as unfair, rehabilitation programs that do not rehabilitate offenders and countless other failures.

To avoid such a trap in the consideration of the criminal phenomenon of identity theft, Utica College's Center for Identity Management and Information Protection (CIMIP) has strived to replace the commonsense approach with a scientific one rooted in the systematic study of actual cases of identity theft. This approach draws from official case procedure records starting at arrest and ending in case disposition. The method is objective and precise and analyzes specific variables and their import, on the road to fashioning an accurate portrait of identity theft characteristics. The broad mission is to use the compilation of study results as a compass by which law enforcers can navigate through the fog of past conjecture to proactively facilitate both original and effective identity theft enforcement efforts. The collection and analysis of such data serves as a wellspring of valuable knowledge, leading to a fuller realization of trends, patterns, and groups perpetrating identity theft. It is the first step toward what is meant to be a successive series of like endeavors gauging the evolution of identity theft as a distinct crime type.

The research center I direct, The Center for Identity Management and Information Protection (CIMIP), is housed at Utica College in central New York, and is a research collaborative of major academic, government and private sector members dedicated to furthering a national research agenda on identity management, information sharing, and data protection. Its ultimate goal is to impact policy, regulation, and legislation, working toward a more secure homeland. CIMIP's advisory board members are committed to working together to provide resources, gather subject matter experts, provide access to sensitive data, and produce results that will be acted upon. But, completing research and publishing papers based on the results is not enough. The results must be put into action in the form of best practices, new policies, regulations, and legislation, training opportunities, and proactive initiatives for solving the growing problems associated with identity theft, the secure sharing of information, and information protection.

CIMIP is a logical outgrowth of Utica College's academic programs and the college's Economic Crime Institute (ECI). Utica College is the forerunner in providing academic programs in economic crime investigation and economic crime management on the undergraduate and graduate levels. Its undergraduate degrees in criminal justice and cybersecurity complete the suite of programs that endeavor to provide government and private industry with a well-educated, cutting edge workforce. Graduates of these programs are currently employed at all

levels in both the private and public sectors. CIMIP's governing body is The Economic Crime Institute of Utica College (ECI); an institute dedicated to leading-edge thinking on economic crime issues faced by business and government through educational programs, policy guidance, research, and solutions. The Institute fosters a learning environment that positions graduates to assume key roles in the fields of economic crime, fraud, and risk management.

CIMIP undertook its most challenging research endeavor with its empirical analysis of over 500 U. S. Secret Service identity theft cases. The goal was to collect investigative case file data from completed identity theft cases spanning from the years 2000 through 2006 and, from this data, document key characteristics of the offense, the offender and the victim. Prior to our study, most of the research findings on identity theft were confined to information submitted by victims through surveys or other forms of victim information submission. While valuable, conclusions drawn from findings were sometimes limited by factors such as variable interpretations of identity theft definitions, did not include incidents unknown to victims, and did not include incidents of crimes against organizations or agencies (e.g., businesses, government). Such surveys were able to only address peripheral characteristics of the offenders and offender modus operandi. Without knowing key information about the offenders, efforts to inform and alert law enforcement and the general public to means to prevent identity theft remained handicapped.

When the study results were first released, they were met with an interesting mix of curiosity and surprise. Contrary to some of the earlier victim surveys, the CIMIP study found that most victims did not know their offenders. The median loss for a case was found to be over $30,000, much more than average estimates drawn from victim surveys (Both findings can be partly attributed to the inclusion of private businesses and public organizations in the study sample). A full one third of offenders were found to have committed their crimes at their place of employment, spotlighting the special problems of unscrupulous "insiders" who would use personal information for criminal purposes. Close to half of the crimes depended upon offenders working in concert.

The results shattered some preconceptions many held about identity theft and identity fraud. The fundamental insight furnished by the study results was that the theft of information used to commit identity fraud was predatory and pervasive, perpetrated by many different types of people from all walks of life. Furthermore, the criminals proved to be patient observers of opportunities that would allow them entrée to source information upon which they could build criminal careers. These identity thieves would settle into a convenient routine of shuttling between the cultivation of data and the conversion of the data into the creation of counterfeit documents and identification cards towards reaching the ultimate goal of the fraudulent use of that data.

The study findings impressed upon me the stark realities of identity theft in our modern society. Many of the crimes were carried out, easily, by individuals using simple forms of scams, trickery, misrepresentation (e.g., phishing), and basic theft (e.g., dumpster diving, mail box rifling) to procure seed information for their later acts of fraud. These were crimes of individual victim manipulation. However, the crimes resulting in the most monetary loss to individuals and businesses alike, proved to be more acts of *system* manipulation committed by loosely

constructed criminal groups exhibiting, in many instances, remarkable skills at exploiting system vulnerabilities. A common characteristic of these cases was the specialization of criminal skills (e.g., paper document experts, laminating experts, check forgers) and the portability of those services depending upon the criminal group's needs. Too often, the individual in control of the criminal "spigot" was the insider, the gatekeeper to personal information of clients and customers.

Through a variety of sources (public service announcements, commercial advertising), United States citizens are periodically reminded about the threats of identity theft and the personal actions that can be taken to help insulate oneself from identity theft victimization. One disquieting story that emerges from the CIMIP study results is that no matter how vigilant we are in following a formula for protecting ourselves from falling victim to identity theft, there is only so much the average citizen can reasonably control. Our personal information is legitimately collected and housed, daily, by numerous private and public sector entities. The successful protection of that information is contingent upon the exercising of robust policies for the safekeeping of it by the information guardians themselves. Absent such policies (e.g., strong employee screening strategies, comprehensive employee monitoring programs), organizations invite attempts at information theft by those entrusted to protect it. Some of the findings of the CIMIP study point to a key threat to identity security as coming from "within"; the insider ready to exploit perceived system vulnerabilities.

The findings that received the most attention after the release of the study can be distilled to the following points separated into four categories: the case, the offenders, the commission of the crime, and victimization. These findings can be helpful in understanding the full extent of identity theft characteristics.

Some notable case characteristics were:

- Cases were referred to the Secret Service from various sources.
    - Approximately 47% were referred by local and state law enforcement agencies.
    - Corporate security and/or fraud investigators referred about 20% of the cases.
- The median actual dollar loss was $31,356.

Offender characteristics showed an interesting diversity.

- Most of the offenders – 42.5%, were between 25 and 34 years of age at the time that the case was opened.
    - The 35 – 49 age group made up 33% of the offenders.
    - 18.5% were between 18 and 24 years old.
    - The remaining 6% were 50 years old or older.

- 24.1% of the offenders were born outside of the United States.
- 71% of the offenders had no official arrest history.
    - Of those who did, a third of the arrests were for fraud, forgery, or identity theft.
- The most prevalent motive of the offenders was personal gain. It took several forms including using fraudulently obtained personal identifying information to:
    - Obtain and use credit
    - Procure cash
    - Conceal actual identity
    - Apply for loans to purchase motor vehicles

The data on the commission of the offenses also proved enlightening.

- In most of the cases, the identity theft facilitated other offenses.
    - The most frequent offense that was facilitated by identity theft was fraud.
    - The next most frequent was larceny.
- Criminal group activity was found in 42.4% of the cases, involving from 2- 45 offenders.
    - The roles that the defendants took varied, but most frequently involved stealing or obtaining personal identifying information and using it for personal gain.
    - In cases with three or more offenders, there is definite coordination and organization, allowing the group to take advantage of criminal opportunities, to create opportunities for crime, and to avoid detection.
- In approximately half of the cases, the Internet and/or other technological devices were used in the commission of the crime.
    - Within the half with no use of the Internet or technology, non-technological methods, such as change of address requests and dumpster diving were used in 20% of the cases.
- The point of compromise for stealing personal identifying information or documents was determined in 274 of the cases.
    - In 50% of those cases a business (service, retail, financial industry, or corporation) provided the point of compromise or vulnerability.

- A family member or friend was the point of compromise in approximately 16% of the 274 cases.

- Approximately a third of the cases involved identity theft through employment.
    - The most frequent type of employment from which personal identifying information or documents were stolen was retail (stores, car dealerships, gas stations, casinos, restaurants, hotels, hospitals, doctors offices) – 43.8%
    - Private corporations were vulnerable to insider identity theft in about 20% of those cases.

The analysis of information on the victims produced some surprises. Although most of the media attention surrounding identity theft and fraud has focused on individuals, they did not make up the largest percentage of victims in this study.

- Over a third (37.1%) of the victims were financial industry organizations: banks, credit unions, and credit card companies.
- Individuals accounted for 34.3% of the victims.
- 21.3% of the victims were retail businesses (stores, car dealerships, gas stations, casinos, restaurants, hotels, hospitals, doctors' offices).
- Victimization of organizations took several forms:
    - The financial services industry was most frequently victimized by offenders using fraudulently obtained personal identifying information to obtain new credit card accounts, to apply for and obtain fraudulent loans, to pass checks, and to transfer funds.
    - The retail industry was victimized by the use of stolen identity information to open store accounts and by purchasing merchandise with fraudulent credit cards.
- The data show that most individuals were victimized by individuals they did not know.
    - 59% of the victims did not know the offenders.
    - 10.5% of the victims were customers or clients of the offender.
    - 5% of the victims were related to the offender.
- 20.3% of the 939 offenders in the cases committed identity theft at their place of employment.

- Of those offenders, 59.7% were employed by a retail business.
- 22.2% were employed by a financial services industry organization.

Knowing the Enemy: Who are the offenders?

As a criminologist, my primary interest in the study results had centered on the offender. My belief was (and still is), that to fully appreciate the threat of identity theft and apply that knowledge to the prevention of future victimizations, one must understand the offenders and how they operate. Just who are these people who commit identity theft and how can this information be valuable to the general public and law enforcement? The quick answer is that they can be just about anyone. But upon deeper inspection, there are some features that underscore what makes them tick; that regardless of age, race or gender, these offenders could all be safely characterized as criminal opportunists in the truest sense. Detailed investigative case notes illustrated that offenders often were thoroughly meticulous in targeting what they perceived as opportunities to commit identity theft and escape detection. The opportunities could arise by chance or by design. In either case, the identity thieves would be alert to taking advantage of these opportunities, opportunities often provided by victims themselves.

While over 70% of the offenders had no arrest history that does not necessarily mean that these offenders had absolutely no criminal history. Statements made by offenders with no official criminal records belie the impression of them as criminal novices. There was some evidence that these offenders could be adept at arrest avoidance. It was clear from the cases studied that more than a few stated they had transitioned over from other crimes (e.g., drug-trafficking) because they believed identity theft was much more lucrative.

Most offenders did not know their victims – only 5% were relatives of victims and 3% were friends/acquaintances of victims. The greater percent of those in which the offender knew the victim involved business/client/employment relationships. Such relationships involved the work of criminally-minded, financial consultants, unscrupulous car dealership employees, unscrupulous loan officers and medical service representatives who valued their financial well-being far more than the health of patients.

Overall, the identity thieves were found to fit into one of three separate criminal categories; *Situational, Routine* and *Professional.* All were found to take advantage of opportunities for crime that were presented to them. One might say that some of these opportunities were presented to them on "a silver platter."

Situational offenders were often those who happened upon opportunities through employment (i.e., "crime at work"). Their jobs were usually ones with access to personal information. Case investigations sometimes revealed these offenders as disgruntled, employees, employees with financial problems, or both. At some point it would dawn upon these employees that they possessed the power to change their lives and act. These offenders would typically use the personal information of others for personal profit for themselves. *Routine* offenders were those with a mindset similar to the situational offender, except that as insiders these offenders decided to act as the "spigot" of stolen personal information that permitted the creation and

evolution of various diverse forms of identity theft that the offender could turn into a continuous criminal enterprise. This type of offender would often move from job to job, with all job positions possessing the element of personal information access. The *professional* identity thief was found to be the most criminally sophisticated of the three types, practicing identity theft as a criminal career. This type of offender could be a solitary offender, but would more likely be the leader of a team, or a "middle manager", usually taking on multiple criminal roles. The professional identity thief was found to wear many hats and participate in diversified criminal activities.

While media reports and commercials have tended to highlight identity thieves preying upon individual citizens, the story that the study tells in this arena is that identity thieves frequently harbor criminal designs much broader in scope. Identity theft attacks against organizations and agencies in private and public sectors were all too common in the sample – with retail and financial services industries taking the brunt of monetary damage. One-third of the cases were found to originate at offender's jobs. As characterized earlier, these crimes were, thus, the work of insiders; those with access to personal information through employment in both private and public sectors. In these cases, the insiders became the criminal wellsprings that triggered a chain of events that would eventually end with the fraudulent use of the stolen information.

Median loss in identity theft cases proved to vary by the size of the identity theft criminal groups. The logical explanation for this was that unless solitary offenders used the Internet as an enabling tool for identity theft commission (and, surprisingly, less than half did), one offender would not "score" as much in terms of profits as if that offender worked as part of a criminal team of identity thieves. The more identity theft foot soldiers fanning out to open new accounts, purchase new credit cards and write more bad checks, the more profits to divide among the criminal group. The insiders with access to information were ideally positioned to act as identity theft ring directors, instrumental in demonstrating the ease of crime commission to potential ring recruits, mentoring them through the first steps of criminal activity and guiding them through methods of exploiting weaknesses in identity protection systems. The final goal being the conversion of stolen identities into fraudulently obtained profits.

Through their own admission, offenders would consistently seek what they saw as the easiest route to potential profits. Time and again, offenders in the study sample proved themselves to be adept at precisely analyzing systems put in place to prevent and deter identity theft. They would search for the weakest links in those systems and devote all their efforts to capitalizing on the exploitation of them. They were prone to specializing their criminal skills. It was common to see identity theft ring leaders erect their identity theft team around the specialized services individual criminal participants could bring to the table. Such skills included expertise in determining the perfect type of paper with which to produce fraudulent checks, or experience in how effectively replicate identifying documents/cards. Some offenders were found to be satisfied with lower profile laminating responsibilities while others would be willing to assume the higher risks of direct fraudulent transactions using the stolen identifications. Together, these specialists would make up the synchronized parts of a fine-tuned identity theft "machine", poised to take advantage of criminal opportunities presented to them.

The offenders were, largely, found to adapt well to control efforts. In some cases, a certain sense of competition with control efforts was palpable. If offenders encountered new adjustments in the system they were trying to "crack" they, would expend extra time and energy to counteract these adjustments. As a group, they were not found to be easily discouraged by technical or systematic roadblocks that might be put in their way. In a word, they often came across as determined. Another criminal quality that emerged was their sense of patience. They could take their time to figure out a new angle in eluding detection and increase their profits. Like 19th century safe crackers, they would often take advantage of connections to other criminals who could help them with new skills to adjust their methods.

Offenders were found to be experienced in isolating "enabling tools" that could make their transition from identity theft to identity fraud all the easier. In over one out of every three cases counterfeit driver's licenses were used in the commission of identity fraud. In each of these cases, offenders were found to be in possession of counterfeit driver's licenses that they had either created themselves, had other offenders create or had purchased from other offenders. These driver's licenses were generated through the theft of personal information from private citizens and were then, in turn, used as the source information for fake driver's license creation to perpetrate the commission of fraudulent acts. The common identity theft case in which counterfeit driver's licenses were used to commit fraud had the following characteristics – 1) involvement of 2 or more offenders acting in concert, 2) the creation and use of multiple counterfeit driver's licenses (often from different states, 3) the use of the counterfeit driver's licenses to purchase business credit cards, open new bank accounts and/or to write counterfeit checks, *and finally* 4) the involvement of at least one "insider" from an organization/agency who provided the "seed" personal information needed as a source for the creation of the counterfeit licenses. While most of these cases could not be characterized as sophisticated organized crime cases, they can safely be said to be examples of organizational crime in that the cases often involved several co-conspirators who developed a system in which personal information was stolen in order to produce counterfeit driver's licenses. The counterfeit driver's licenses would serve as a catalyst to a chain of events in which offenders would use the fake licenses as "authentication" for the opening of bank accounts and the purchase of credit cards used to commit fraud.

While the original methods of personal identification theft could be quite primitive (e.g., dumpster diving, mailbox theft), a reoccurring characteristic in driver's license identity theft cases involved an insider with access to personal identification through employment. In some cases, the insider was an employee of an organization with direct access to personal information of customers/clients/patients (e.g., banks, hospitals, telecommunication firms) who participated in the actual acts of identity fraud as part of a conspiracy or "ring". In other cases, the insider did not participate in the identity fraud acts directly, but sold the information to facilitate the creation of the fake driver's licenses (e.g., employees of automobile dealerships). In either scenario, the personal information stolen was converted, directly, into the manufacturing of counterfeit driver's licenses to be used for identity fraud. Some created drivers licenses themselves with software and materials like paper and ink purchased from office supply stores. Others knew individuals who specialized in creating fake driver's licenses and sold their specialized services.

In the final analysis, the seasoned identity thief, would take the path of least resistance toward the ultimate goal of using someone's identity to commit fraud in that person's name. The enabling tools became vulnerabilities in the systems or individual protections against identity theft victimization. Often these vulnerabilities were cases in which the system let the individual down. The following are a list of examples of these vulnerabilities, or "points of compromise", that emerged from the CIMIP study:

Merchant recognition of counterfeit cards – Failure of merchants to detect that credit cards were not authentic (e.g., manufactured by the offender using victims' personal identification information).

Individual victim oversight – Failure of the individual victim to protect or insulate source of information used by offender to assume the victim's identity in the commission of fraud against the victim. Includes instances of source information obtained by acquaintances/relatives through direct contact with victim, "dumpster diving," mail theft

Bank oversight of new account creation – Failure of bank personnel to recognize false identification information presented by offenders to open new accounts in victims' name.

Oversight of employee access to customer/client information – Failure of employer to effectively monitor employee use of customer/client personal information

Credit card issuers' oversight of adding users to existing accounts – Failure of issuers to effectively verify authenticity and victim approval of request to add offender to existing account as a credit card user.

Government recognition of altered forms – Failure of government agency to detect false documentation leading to fraudulent misuse of documents in victim's name.

Oversight of employee access to client/customer credit cards (skimming) – Failure of employer to effectively monitor employee use of credit cards in the course of legitimate credit card transaction.

Basic offender characteristics of identity theft offenders, then, are the following –

Identity theft offenders:

- Are "Criminal opportunists"
- Search for the easiest route to profits (e.g., testing methods)
- Specialize criminal services
- Adapt their abilities to control efforts
- Are patient

- Prize the special role of criminal "Insiders"
- Often depend on the creation and use of fake driver's licenses as catalysts for identity crimes

Applying Results to Victim Protection: Optimizing Victim Protections

How does this empirical information translate into assistance to the victims of identity theft? In my opinion, the results highlight the responsibilities we all have to optimize basic protections of our citizens from falling victim to identity thieves and making sure victims are properly treated if those protections ever fail. For too long, we have accepted a less than adequate approach in at least two areas that could help cut off some "points of compromise" (and help prevent identity theft) and one area that could advance our efforts toward making certain that we truly support the "first responders" to the crimes and, thereby, treat identity theft victims properly. While I am sure there are more, I have distilled my recommendations to three optimized protections; Optimized Authentication Protection, Optimized Protection of Personal Information and Optimized Protection by Law Enforcement.

Optimized Authentication Protection

Empirical research has demonstrated that identity thieves (especially *professional* identity thieves) look for soft spots in systems that, when exploited, pay the biggest dividends to them through the use of stolen identities to commit fraud. One of the simplest ways for offenders to commit fraud using stolen identities is to open new credit card accounts in the names of victims. Both individuals whose identities are stolen and merchants become ultimate victims. The gatekeepers to identification approval are often those who are not optimally equipped to effectively discern the authenticity of identification documentation. These individuals become unwitting conduits for criminality by opening the door to identity fraud. In some cases, security measures built into authenticating documents are less than adequate.

Types of authentication employed daily range from being quite simple to being quite complex. A commonality, though, is that the methods used can vary among the entities represented by the authentication "readers" (e.g., law enforcement, retail, transportation) and jurisdictions within which the readers operate. Key dependent factors include skill levels of the readers and the tools the readers employ. CIMIP supports the work done in this area by groups like the American National Standards Institute, the North American Security Products Organization and the Document Security Alliance. It is recommended that government support further efforts that would facilitate a series of reader applications of the testing methods throughout the U.S across relevant testing entity groups. Such applications should entail physical applications of methods along with qualitative surveys on the level of ease and reliability of the applications. Results of the applications should be integrated into national standards for authentication testing to set the stage for the enhancement of authentication methods aimed at narrowing the scope of criminal opportunities that now exists for identity thieves. Both the private sector and government must work closely together to optimize the capabilities of

authentication readers, ensure they are properly trained and guarantee that that the most effective security layers are installed onto identification documents.

Optimized Protection of Personal Information

Much of the average citizen's personal information is legitimately housed by numerous private sector businesses and government agencies in our modern society. It is a sign of progress and affords us with many services and conveniences that we would not ordinarily have. With regard to identity theft, these services and conveniences can come with a heavy price if optimized protections are not installed to prevent personal information from becoming compromised and used as the source for the selling of it to commit identity fraud. While much societal attention has been paid to invasions of information systems from the outside, the danger of breaches from the "inside" has not received as much scrutiny. Yet, as pointed out in CIMIP's study of identity theft case characteristics, cases in which those given access, through employment, to personal information often result in those entrusted with protecting this information becoming the architects of rings dedicated to creating and sustaining criminal careers in identity fraud. It is time that the public and private organizations housing this source information are held to a higher standard to prevent these insider breaches, cutting off the criminal lifeblood that effects so many victims of identity theft and identity fraud.

As recommended by scholars like Jeffrey Stanton in research on the importance of employer responsibility in ensuring that personal information of customers and clients is protected from exploitation, managers in the public and private sectors must see to it that the proper climate is set to prevent such actions. Ingredients for optimized prevention include: 1) effective employee screening methods at hiring; 2) effective monitoring/surveillance of employee activities in both the real and virtual settings; 3) limitation of data access to only select employees; and 4) the establishment and public notification of employer policies on employee interaction with data and the repercussions/penalties for violations

Optimized Protection by Law Enforcement

There are a number of agencies that are responsible for identity theft control on a national level including the U. S. Secret Service, the Federal Bureau of Investigation, the U.S. Postal Inspection Service and U.S. Immigration and Customs. These agencies field direct reports from victims and others reporting identity theft, or what is thought to be identity theft. The agencies also work closely with state and local law enforcement agencies in addressing identity theft, often interfacing with identity theft task forces that combine the efforts of local, state and federal agencies. Studies like the one completed by CIMIP also demonstrate that state and local law enforcement agencies play a significant role, one that can easily go unnoticed by the general public due to the media profile given to larger "dollar loss" cases that are typically handled by federal enforcement agencies. Every day, municipal police, county police/sheriff's officers and state police are instrumental in the successful detection and investigation of numerous identity theft cases. In many instances, they represent the first public officials who are made aware of the offenses or put in the position of determining if examined evidence would lead to a conclusion

that identity theft has occurred. As such, they are frequently the *first responders* to identity theft victims.

Based upon the analysis of CIMIP's data, it appears that local/state enforcement officers involved in the identity theft cases were quite sensitized to identity theft enforcement. They went the extra yard to piece together information that would end in a clear picture that identity theft had occurred. It is important to note that the sample is a study of those who *did* detect and properly investigate the offenses as identity theft. It is for precisely that reason that this information is used for the basis of an informative report on experiences and desired procedures. Being sensitized to signs of identity theft is as important to a local enforcement officer as telltale signs would be to an emergency medical technician at the scene of an accident or to an auditor investigating the records of a corporation plagued with financial inconsistencies. Being a first responder, it rests with the local officer to determine if the "surface" offense is in fact the only offense that has taken place in a given investigation. A sensitized first responder would be able to skillfully dig beneath the surface and acknowledge the crime of identity theft, one that may have never been unearthed without the officer's special skills.

While the CIMIP study underscored the work of local law enforcers who clearly represented what should be done to effectively respond to identity theft victimization, other evidence has suggested that sensitization to identity theft recognition and investigation is not always as routine as one might expect. In his recent study of local law enforcement and identity theft, Vern McCandlish points out areas in which local enforcement is either lacking or requires improvement. They include: 1) formal written policies specific to identity theft response and investigation; 2) follow up contacts of victims; 3) the provision of copies of the written reports taken by the officers to the reporting victims; 4) utilization of the Federal Trade Commission's Identity Theft Affidavit, an affidavit created by the Federal Trade Commission, in cooperation with the financial industry, designed to assist identity theft victims in recovery (Once completed, the affidavit allows the victim of identity theft to have one form that can be submitted to any business to detail the facts of the victimization and can be reused with different agencies .The victim is not required to complete a separate custom form for each business contacted to correct the errors caused by the identity thief); 5) written policies of entering the reported incident of identity theft into the Federal Trade Commission's clearinghouse database; and 6) an emphasis on the importance of the police first responder empathizing with the victim.

To optimize swift and effective local law enforcement responses to victims of identity theft, it is strongly recommended that government infuse resources into "best practices" training programs designed to build upon lessons learned from effective federal, state and local law enforcement strategies and direct those programs, widely, to local law enforcement officers throughout the nation. McCandlish's research highlighted the following areas that are vital for the police first responder to have proper training in when responding to the victims of identity theft:

- The language of the criminal statutes
    - Criminal liability
    - Jurisdictional issues

    - Victim's rights

- Criminal objectives in obtaining and using personal identification information
- What information constitutes personal identifying information and what risks result from failure to properly secure this information
- The true levels of stress and emotional trauma the victim is dealing with
- The basic needs of the victim
- The importance of documenting the complaint in a written report
- How to offer basic advice on self protection when fielding questions from citizens or the press
- Approaching the victim in a manner that does not leave the victim feeling to blame for being victimized or failing to empathize with the victim
- Exhibiting appropriate compassion for the victim's plight

Final Thoughts

The early research work done by CIMIP has documented both qualitative and quantitative features of identity theft that can logically be transformed into suggestions for policy change to help limit future victimizations and improve system treatment of victims. Firms like The Santa Fe Group have been instrumental in pointing out specific needs that must be addressed to provide effective service to victims. An obvious way in which we can lessen the burden of identity theft is to clear away any obstacles that may impede the ability of the victim to restore his/her identity to a pre-identity theft level. In essence, this would amount to the victim receiving a "clean record", devoid of false charges that may have resulted from the victimization. Another way to lessen the burden is to support state and federal efforts to make it easier for victims to receive restitution as a result of their victimizations. CIMIP research of criminal case sentences found that restitution was imposed in only a minority of the cases analyzed. Clearly, this trend must change if victims of identity theft are to be afforded the services and protections they deserve. To ensure that identity theft cases are pursued to the fullest extent of the law, criminal prosecutions must be aggressive and effective. National prosecution associations like the National Association of District Attorneys (NDAA) and the National Association of Attorneys General (NAAG) should be supported in any efforts to emphasize the urgency of the prosecution of identity theft and provide requisite training to enhance prosecutors' abilities to prosecute effectively.

But, an improvement area that we must be careful to not overlook is the importance of educating the public on the finer points of doing everything one can to prevent identity victimization to begin with. Experts in identity theft prevention, like Martin Biegelman, have pointed out simple practices that can be followed that can dramatically reduce the risk of

becoming an identity theft victim. These practices include safeguarding social security numbers, minimizing the amount of personal information one carries, reducing the sharing of personal information and being alert to credit card skimming tactics. They also include simple computer use practices like enabling strong password protection, encrypting files and being alert to common phishing and related scams. The general public should understand actions that can be taken to limit the extent of identity theft victimization through early recognition of it by practicing the routine review of personal credit reports, monthly financial statements and social security earnings and benefits statements. Improved prevention education must be matched with education in the steps that can be taken in expunging victim names and information from criminal justice databases.

In short, it should be the obligation of both the public and private sectors to team together to support, development and implement sound and comprehensive public awareness programs designed to facilitate a precise understanding of how to help insulate oneself from the pain of identity theft victimization. In studies conducted on identity thieves' accounts of their own criminal lives the message is clear; identity thieves believe that stealing identities is "easy" because so many of us make it easy for them to commit. It must be the mission of government to make it as difficult as possible for identity thieves to commit their criminal acts. Getting the "word" out to the average citizen is an important step in that direction

I would like to thank the Subcommittee for its time today. I appreciate the opportunity to discuss this important issue.