INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

TESTIMONY

Statement of

Chief Mary Ann Viverette
Third Vice President

Of the
International Association of Chiefs of Police

Regarding
Fighting Identity Theft

Before the
Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
U.S. House of Representatives
June 24, 2003

515 N. WASHINGTON STREET
ALEXANDRIA, VA 22314
703-836-6767
WWW.THEIACP.ORG

Good Morning, Chairman Bachus, Representative Sanders and Members of the Subcommittee.

I am pleased to be here this morning on behalf of the International Association of Chiefs of Police (IACP). As you may know, the IACP is the world's oldest and largest organization of law enforcement executives, founded in 1894, and with a current membership exceeding 19,000. Our mission, throughout the history of our association, has been to address urgent law enforcement issues and to develop policies, programs, training and technical assistance to help solve those issues. And as I appear before you today, the issue of identity theft is one of great and growing concern to the law enforcement community. In a relatively short period of time identity theft has transformed from a relatively unnoticed crime to a major problem in the United States and around the world.

Growth of Identity Theft

As you know, identity theft is the wrongful use of another's personal information, such as credit card numbers, Social Security number, and driver's license number to commit fraud or another form of deception. This is usually done for monetary gain, although there may be other motives.

The target of identity theft is information that will enable the thief to assume another's identity for a criminal purpose. In the last few years, personal information has become one of the commodities most sought after by criminals in this country and elsewhere. Because it is usually part of a larger criminal enterprise, the theft of personal information is one of the most serious of all crimes.

Although identity theft is in itself a criminal act under both federal and most state laws, the theft is almost always a stepping-stone to the commission of other crimes. Typical crimes associated with identity theft include credit card fraud, bank fraud, computer fraud, Internet fraud, fraudulent obtaining of loans, and other schemes designed to enable the perpetrator to profit from the original theft.

Furthermore, funds obtained illegally as a result of the identity theft and its resultant frauds may be used to finance other types of criminal enterprises, including drug trafficking and other major forms of criminal activity.

The escalation of identity theft in the United States is due in large part to the technology revolution that has brought the country into the so-called Information Age. The vastly expanded use of computers to store personal data and the growing use of the Internet have provided criminals with new incentives and new means to steal and misuse personal information. As the use of technology to store and transmit information increases, so too will identity theft. Consequently, identity theft will likely become an even greater problem in the future.

Impact of Identity Theft

The ability to accurately define the financial losses of the vast number of crimes committed by means of identity theft is not possible at this time. Many identity theft crimes are not reported to police, and there is no single source of information on this issue. It is fair to say, however, that the cumulative financial losses from identity theft and the various crimes that feed from it are staggering.

However, perhaps even more tragic than the monetary loss is the personal cost of identity theft. Because identity theft by definition involves the fraudulent obtaining of funds in the name of someone else, the victim of identity theft may sustain not only great financial loss, but also severe damage to credit standing, personal reputation, and other vital aspects of the victim's personal life. For example, the victim may suffer garnishments, attachments, civil lawsuits, and other traumatic consequences stemming from the identity theft. In some cases the victim may be forced into bankruptcy, further damaging his or her reputation and credit. In other instances, the victim may become subject to criminal prosecution because of crimes committed by the perpetrator of the identity theft in the victim's name.

Even if the victim ultimately clears his or her credit records and avoids other personal and financial consequences of identity theft, the physical and mental toll on the victim can be significant. Typically, a victim of identity theft will spend months or years trying to clear his or her credit records. Many hours of difficult and stressful effort are often necessary, because the merchants and institutions that have been defrauded in the victim's name are not easily persuaded that the victim is innocent of any wrongdoing. The frustration and distress engendered by this heavy burden often take a significant toll on the mental well being and physical health of the victim. And, worst of all perhaps, the victim's efforts to clear him or herself may be unsuccessful, leaving the victim under a cloud for the rest of his or her life.

Types of ID Theft and ID Theft Operations

As has been noted, the key target of identity theft perpetrators is personal and confidential information of individuals. There are so many methods by which identity thieves may acquire personal information that it is impossible to catalog them all here. However, the following methods are commonly used:

- Stealing wallets and purses containing personal identification, credit cards, and bank cards.
- Stealing mail, including mail containing bank and credit card statements, preapproved credit card offers, telephone calling cards, and tax information.
- Completion of a false change-of-address form to divert the victim’s mail to another location.
- Searching trash for personal data found on such discarded documents such as preapproved credit card applications or credit card slips discarded by the victim.
- Obtaining credit reports, often by posing as a landlord, employer, or other person or entity that might have a legitimate need for, and right to, credit information.
- Obtaining personal information at the workplace or through employers of the victim.

- Discovering personal information during physical entries into the victim's home. Such entries may be unlawful, as in burglary, or initially lawful, as when friends, service personnel, or others are invited to enter the home.
- Obtaining personal information from the Internet. This may be information stolen by hackers or freely provided by the victim in the course of making purchases or other contacts.
- Purchasing information from inside sources such as store employees, who may for a price provide identity thieves with information taken from applications for goods, services, or credit. At least one instance has been reported of an employee of a credit bureau collaborating with identity thieves to provide personal information from credit bureau records.
- *Pretexting*, in which a thief telephones the victim or contacts the victim via Internet and requests that the victim provide personal information
- *Shoulder surfing*, a practice whereby the thief positions himself or herself near a victim in order to obtain personal information by overhearing the victim or seeing the victim's actions. For example, the thief may stand near a pay telephone in a public place and listen as the victim gives credit card number information or other personal information in the course of making a call. Similarly, thieves may loiter near an automated-teller machine (ATM) and visually observe the victim keying in password numbers on the machine.
- "Skimming," which is the electronic lifting of the data encoded on a valid credit or ATM card and transferring that data to a counterfeit card. There are many variations of this practice. For example, an identity thief may recruit an employee of a retail store, restaurant, or other retail establishment. The employee is provided with a hand-held electronic device that can read data from a person's credit card when the consumer presents it to the employee. The collusive employee then surreptitiously "swipes" the credit card through the hand-held "reading" device, which records the electronic data from the card. The employee then returns the device to the thief and the thief extracts the recorded data from the device.

- Identity thieves may also purchase personal information about potential victims from persons or entities that routinely collect such information. In some instances these entities may be legitimate, but in many cases they are criminal enterprises formed for the specific purpose of selling information to thieves.

How Stolen Information is Used

There are literally hundreds of ways in which identity thieves may use the information they have stolen. The following are just a few examples:

- Once they have a victim's credit card number, thieves may call the victim's credit card issuer and, pretending to be the victim, asks that the mailing address on the account be changed. The thieves then run up high charges on the credit card, and because credit card statements are no longer being sent to the victim's real address, the victim might be unaware of what is happening for weeks or even months.
- These same thieves who have obtained a victim's credit card information may also request that the credit card company send them credit card "checks," which are written for cash just as are bank checks. Again, the charges are unknown to the victim because the credit card statements are no longer coming to the victim's address.
- Having obtained personal information such as name, date of birth, Social Security number, and so on, the thieves open new credit card accounts in the victim's name and run up charges until the victim becomes aware of the fraud. Similarly, credit accounts may be opened at stores using the victim's identity.
- The thieves open bank accounts in the victim's name and write bad checks on the account.
- The thieves obtain loans, such as real estate, auto, or personal loans, using the victim's identity.
- The thieves counterfeit checks or debit cards, and drain the victim's bank accounts of funds.

- The thieves establish services such as utility, telephone, or cell phone service in the victim's name.
- The thieves make long distance calls using stolen credit card numbers.
- The thieves may obtain other goods and privileges by using the victim's identity and information, either in person or by telephone or via the Internet.

These are only a few of the numerous schemes that an identity thief may use to obtain money, goods, or services at the expense of the unwitting victim.

Perpetrators

Identity theft is not perpetrated only by so-called white-collar thieves. It is committed by criminals of all types. A recent report indicates that during the period November 1999 to March 2001, about 12 percent of all suspected perpetrators reported to the Federal Trade Commission had a personal relationship of some sort with the victim. However, the remaining 88 percent of suspects had no relationship to the victim of the theft. Thus, while the thief may be a family member, a coworker, a friend, or someone else personally known to the victim, in the vast majority of instances the perpetrators are unknown to the victim.

In most cases the thieves are geographically located far from the victim's place of work or residence. These perpetrators may be solo operators, but more often are members of a larger criminal organization. Such organizations may be local, regional, national, or international in scope. They may be composed of specific ethnic or national groups, or may be simply a collection of criminals of various backgrounds cooperating to obtain illegal profits at the expense of the innocent victims.

Law Enforcement Response

In earlier years, the involvement of local police departments in identity theft cases was typically minimal. In fact, many local police departments refused to take complaints about identity theft because the crime was not well understood. This was caused by several factors, including the lack of state laws making identity theft a crime, the fact that most identity theft operations are multi-jurisdictional enterprises, with perpetrator and

victim usually widely geographically separated, and the general lack of police expertise in investigating the crime of identity theft.

Fortunately, this situation is now rapidly being remedied. The passage of numerous federal and state statutes has given federal, state, tribal and local law enforcement agencies the authority to investigate and prosecute identity theft crimes, and departments everywhere are becoming more aware of the significance of identity theft and the availability of the means to combat it.

However, since identity theft and its resultant crimes often involve a wide variety of offenses and means of committing those offenses, effectively combating identify theft will require not only the dedication of significant resources but also greater collaboration and cooperation between federal, state, tribal and local law enforcement agencies. This information sharing among agencies is essential as it may not only lead to a successful prosecution of the case in one jurisdiction but concurrent investigation in other areas of the country. I am pleased to say that in recent years, federal, state, tribal and local law enforcement agencies have made significant strides in this area and are increasing our capability to investigate, track, apprehend and prosecute these criminals.

Nevertheless, the law enforcement community cannot effectively combat identity theft by itself. Citizens need to take proactive steps to protect their personal information. Businesses must act to establish safeguards that will ensure that the personal information of their patrons is not exposed. Policy-makers at all levels of government need to review current statutes to ensure that protection of personal information is a priority and develop legislation that will strengthen the penalties for identity theft.

Only by acting to establish greater protections of personal information and by aggressively tracking down and punishing those who commit identity theft can we hope to turn the tide in this battle.

This concludes my statement. I will be glad to answer any questions you may have.