

**Statement of Daniel L. Mihalko, Inspector in Charge  
Congressional & Public Affairs  
Of the  
United States Postal Inspection Service  
On Fighting Identity Theft  
And the  
Role of the Fair Credit Reporting Act**

**Before the  
Financial Institutions and Consumer Credit Subcommittee  
of the  
Financial Services Committee  
U.S. House of Representatives**

**June 24, 2003**

Mr. Chairman and members of the Subcommittee: thank you for holding this hearing on the topic of identity theft, America's fastest growing crime. I appreciate the opportunity to discuss the subject of identity crimes and related fraud, and the role of the United States Postal Inspection Service in combating this rapidly growing menace.

**Role of the Postal Inspection Service**

The U.S. Postal Service delivers more than 200 billion pieces of mail a year, containing money, messages, and merchandise, to 138 million addresses at some of the most affordable postage rates in the world. U. S. Postal Inspectors are mandated to safeguard all of it—including the people who move it and the customers who use it.

Congress empowered the Postal Service “to investigate postal offenses and civil matters relating to the Postal Service.” Through its security and enforcement functions, the Postal Inspection Service provides assurance to American businesses for the safe exchange of funds and securities through the U.S. Mail; to postal customers of the “sanctity of the seal” in transmitting correspondence and messages; and to postal employees of a safe work environment.

As one of our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, the United States Postal Inspection Service has a long, proud and successful history of fighting criminals who attack our nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public.

Postal Inspectors work closely with U.S. Attorneys, other law enforcement agencies, and local prosecutors to investigate postal cases and prepare them for court. There are approximately 1,900 Postal Inspectors stationed throughout the United States who enforce roughly 200 federal laws covering investigations of crimes that adversely affect or fraudulently use the U.S. mail and postal system.

Last year, U.S. Postal Inspectors made more than 11,000 arrests, over 6,000 of which were related to mail theft. One-third of those 6,000 involved identity theft. In the first eight months of our 2003 fiscal year, we have already exceeded the number of identity theft arrests made throughout all of last year.

### **What is Identity Theft?**

Identity theft occurs when a thief steals key pieces of someone's identifying information, such as name, date of birth, and Social Security number, and uses the information to fraudulently apply for credit or to take over a victim's credit or bank accounts. Identity theft occurs in a variety of ways. Those that involve the use of the mail receive swift and aggressive action by Postal Inspectors. We ensure that consumers are being protected. In addition, we work with the mailing industry to develop best practices on how best to design mailing pieces to prevent identity theft. Our collaboration with the mailing industry is another example of how the industry as a whole is serious about the issue and working to stay on top of it for the benefit of consumers. Mail is important to consumers who receive it and to the businesses that send it.

### **Tactics Used by Identity Thieves**

In the past, pre-screened credit solicitations were more vulnerable to identity theft because they simply required the customer to sign the solicitation and return it. When the items were stolen from the mail, they presented a risk to the consumer. But now credit card companies have begun automatically discarding such applications when they are returned with a change of address. Actions by the industry have made these mailings less attractive to the identity thief.

Identity theft is continuing to evolve with the expansion of the Internet and other electronic means. The mail is no more vulnerable than other sources of personal information, such as corporate and government records and computer databases. Financial institutions have implemented many safeguards to reduce the likelihood that personal financial information found within the mail can be stolen. The Postal Service is continually working to improve the security of the mail, and Postal Inspectors are making great strides in apprehending those who would use the mail to further their crimes.

Identity fraud is digging deep into consumer's pockets -- millions of dollars were lost in the past year by financial institutions and victims across the country. Thieves use a variety of tactics to drain a victim's finances, including stealing mail; posing as a loan officer and ordering your credit report (which lists account numbers); "shoulder surfing" at the ATM or phone booth to get your PIN code; and "dumpster diving" in trash bins looking for credit applications, canceled checks or other bank records.

Until a few years ago, a thief could submit an address change to divert customers' mail without their knowledge. Usually, redirected mail is sent to a commercial mail receiving agency in an attempt to ensure the perpetrator's anonymity. In response to recommendations by the Chief Postal Inspector, a prevention measure that addresses fraudulent change-of-address orders was adopted by the U.S. Postal Service. Post Offices now send a "Move Validation Letter" to both the old and new address when a change is filed. The letter instructs an individual to call an "800" number if a change was not filed. This simple measure has virtually eliminated the use of placing a false change-of-address order with the Postal Service as an avenue for committing identity theft.

### **Impact on Victims**

One of the most insidious aspects of identity theft is the length of time the scheme is carried out before it comes to anyone's attention. It may be months before a victim realizes they've been targeted. It's not until a consumer gets turned down for credit, a car loan, or a mortgage on a dream house because of a bad credit rating—knowing they've paid their bills—do they begin to realize what has taken place. Most victims do not learn about the theft of their identity until 14 months after it has occurred. More than half of the victims we interviewed report their cases have been open, on average, 44 months. They also reported that, as victims, they spent, on average, 175 hours actively trying to restore their credit and "to clear their good name."

Identity theft can do more than ruin a person's credit; it can cause more serious damage. Identity theft hurts a victim in two ways. At first a victim must deal with the obvious financial issues. The second, hidden, factor is the emotional one: having to deal with privacy and practical issues such as a credit history that isn't theirs. The problem doesn't go away with a few phone calls -- it can stick with a victim for a long time. That's why it's such a serious issue. Victims run the gamut of society, they're wealthy, they're poor, they're old, and they're young. Anyone can become a victim.

In a recent Postal Inspection Service investigation based in Chicago, Illinois, the destructive activities of an identity thief resulted in the loss of thousands of dollars and the death of a primary victim. This scheme began in July 1999 when the identity thief began dating the estranged wife of a Chicago resident. Without his knowledge, the wife assisted the thief in stealing her former spouse's identity by providing the thief with the spouse's personal information.

In January 2000, the spouse filed a complaint with the Chicago Police Department after realizing that he was a victim of identity theft with losses exceeding \$200,000. In February, the spouse received a package from the thief wrapped as a FedEx delivery. After holding the package for several days, the spouse received a voice mail message from the thief indicating the package was a gift. As he sat in his living room, he opened the package, which exploded, killing him instantly.

Last year a colleague of mine learned about identity theft the hard way. His bank called him in April last year and asked if he had authorized a \$4,500 cash advance on his credit card in Miami, Florida that day.

He was stunned. The bank had called only hours after the withdrawal was made, following an alert initiated because certain account parameters indicated something might be wrong. Luckily for him, the bank simply asked that he sign an affidavit that he had not been in Miami and hadn't made the withdrawal. He wasn't held liable for the money. And he never found out what ID the thief had used to get access to his account.

Unfortunately, my colleague's ordeal wasn't over. He received a call a few months later from a cellular phone company, asking if he'd opened an account with them in Miami. Someone had racked up \$1,800 in calling charges under his name and then disappeared. Once again, he signed an affidavit disclaiming knowledge of the charges, and the account was cleared. This time, he called the three main credit bureaus and reported the fraud.

My colleague is just one of hundreds of thousands of individuals who are victimized each year. The culprits may be found among employees (or patrons) of mailrooms, airlines, hotels or personnel offices--anyone who has access to a person's financial information. They can use your credit card or instead use encoding equipment, sold by business supply companies, and blank cards with magnetic strips on the back, to encode your account number onto a counterfeit card with a different name. Thieves sometimes seek jobs specifically to get access to financial information; alternately, they may bribe employees in such positions to supply them with the data they want.

The problem is compounded by the ease with which a phony ID can be obtained. On the Web are scores of sites with complete instructions on creating a "new you." Personal computers, "scanners" and color printers (or copiers), all facilitate creating false identification documents.

### **Commitment of Resources and Jurisdiction**

Because identity theft crimes can involve the use of the mail, the U.S. Postal Inspection Service has become a lead agency in investigating these crimes. Even in cases where the original theft does not involve the mail, the mails may be used to send the credit cards to a commercial mail receiving agency or alternate

address. That's why Postal Inspectors are involved in investigating this crime and take it so seriously.

Each of the Inspection Service's 18 field divisions investigates identity theft within their respective boundaries. Identity theft investigations are reported, categorized, and tracked in an Inspection Service national database used by management to coordinate the appropriate investigative response. During the past few years, Inspection Service resources devoted to identity theft investigations have increased significantly – by 38 per cent.

As the resource commitment increases, so have the number of arrests. In 2001, we made 2,097 arrests; in 2002, 2,243. As of May of this year, we've made 2,264 identity theft arrests. Keep in mind this is in the context of 200 billion pieces of mail the Postal Service handles annually. But we take this crime seriously because of the impact on its victims. Due to our efforts, the mail may be one of the most protected mediums where identity theft is investigated and prosecuted.

### **Identity Theft Investigations**

In a typical case this year, Postal Inspectors arrested eight West African nationals who were operating a multimillion-dollar counterfeit and stolen credit card enterprise nationwide. And Postal Inspectors in New York arrested 16 members of a gang that ran a passport photo business, supplying false identifications for cashing checks stolen from the mail.

Last week Postal Inspectors announced the results of a round-up of 103 mail thieves throughout the western United States. A multi-agency task force comprising U.S. Postal Inspectors, members of the U.S. Marshals Fugitive Apprehension Strike Task Force, U.S. Secret Service, state and local police, and the Northern California Identity Theft Task Force targeted mail thieves in California and Nevada. Similar operations took place in Arizona, Hawaii, Utah and New Mexico. Federal and state prosecutors are supporting the work of the task force by aggressively prosecuting individuals involved in mail and identity theft.

Here are just a few examples of identity theft cases investigated by Postal Inspectors in the past year. In Detroit, Postal Inspectors investigated a gang of mail theft recidivists who were recruiting street people, called "runners," to obtain cash advances from banks and casinos via credit cards. Inspectors executed a search warrant at the residence of a suspect in January 2002 and recovered more than 180 documents listing victims' personal IDs. Inspectors and agents from the Detroit Metro Identity Theft Task Force identified and arrested the ringleader of the group who, at the time of his arrest, had more than 700 car rental applications with names, dates of birth, Social Security numbers, and credit card accounts of potential victims. The ringleader and a cohort reportedly called credit card issuers, purporting to be the true account holders, and requested that replacement credit cards be mailed to them. The car rental manager who supplied the rental applications and an employee who worked at a

health plan office were later indicted for providing documents to the gang. Total fraud losses exceeded \$700,000.

An Illinois man was sentenced last year to 25 months in prison and ordered to forfeit \$590,000 in assets to banks after pleading guilty to the unlawful possession of an access device, mail fraud, and bank fraud. A joint investigation by Postal Inspectors and special agents of the Social Security Administration determined he had fraudulently applied for more than 200 credit cards using numerous victim IDs.

Postal Inspectors in Jacksonville, Florida, arrested six people believed to be running a major identity theft ring. The arrests were the result of a joint investigation by the Northeast Florida High Tech Task Force, which includes Postal Inspectors, members of the Jacksonville Sheriff's Office, and several other federal, state, and local law enforcement agencies. Victims of the ring included employees of the Winn-Dixie Corporation and Hollywood, Florida, police and fire departments. The six suspects were charged with 44 counts of violations related to the Racketeering Influenced Corrupt Organization (RICO) Act, including criminal use of personal information, grand theft, organized fraud, and manufacturing fraudulent IDs. On May 27, 2002, one of the suspects pled guilty to RICO violations and related charges.

Las Vegas police arrested a man last year for "driving under the influence" and later discovered he had an outstanding arrest warrant for identity theft in Arizona. Phoenix Postal Inspectors reported he stole a person's Social Security number, applied for numerous credit cards in the victim's name, and had the cards mailed to a box he rented at a commercial mail receiving agency. Postal Inspectors and Secret Service agents searched the man's business and discovered numerous fraudulent documents.

### **Statutes Used in Identity Theft Cases**

A number of statutes enable us to take action against identity theft involving the use of the mail. Under Title 18, U.S. Code, Section 1708, Postal Inspectors may arrest individuals for the possession of stolen mail or filing a false change-of-address order; the penalty is a \$2,000 fine or up to five years' imprisonment, or both. In 1998, the Identity Theft and Assumption Deterrence Act of 1998, was signed into law. This law expanded the scope of the identity fraud statute (18 U.S.C. § 1028), and made it a federal crime for the unauthorized use of personal identification in the commission of any federal law (felony or misdemeanor), or a state or local felony.

But one of our top weapons in the fight against identity theft is a statute originally enacted over 125 years ago: the criminal mail fraud statute. If someone applies for a credit card in your name, perpetrators may be prosecuted under Title 18, USC 1341. The penalty is a \$1,000 fine or up to five years' imprisonment, or both--unless a financial institution is affected, in which case the fine may be raised to \$1 million and imprisonment for up to 30 years. The public policy that underlies this statute remains valid today: *The postal system created by*

*Congress to serve the American public should not be used to conduct schemes that seek to cheat the public.*

Our experience demonstrates that enforcement laws, coupled with an aggressive education campaign, industry cooperation, interagency enforcement efforts and preventive/security measures described below, are invaluable tools in the arsenal of law enforcement.

### **Interagency and Industry Cooperation**

To address the fundamentals of identity theft, the Postal Inspection Service works diligently with the credit card industry, financial institutions and other law enforcement and regulatory agencies. In 1992, the Postal Inspection Service sponsored its first Credit Card Mail Security Initiative meeting in Washington, DC. We continue to promote and host these semi-annual meetings.

Many of the preventive strategies discussed at our meetings have been implemented by our financial industry partners, and have resulted in reduced losses attributed to mail theft and the subsequent identity theft that occurs from it. The now-common concept of credit card activation was first proposed by a Postal Inspector and was promoted through the Credit Card Mail Security Initiative meetings. The industry embraced and implemented this prevention strategy, which resulted in the reduction of significant industry fraud losses over the past decade.

In addition, working in conjunction with industry partners, Postal Inspectors analyze information from credit card thefts to identify “Hot Spots” for investigative attention. The Postal Inspection Service notifies the financial industry of zip code areas suffering abnormal losses, so they can take extra precautions when mailing to those areas.

Thanks to the collaborative efforts between the Postal Inspection Service and its working-group partners, we are beginning to see the results of this and many other fraud prevention initiatives. In addition to modifying industry practices, our collaboration has produced a number of fraud prevention guides, including the Fraud Detection and Reference Guide; Account Takeover Prevention Guide; and Detecting and Preventing Credit Application Fraud. The working group was also responsible for the Identity Theft Consumer Awareness video and the Identity Theft brochure. At the conclusion of my testimony, I have included prevention tips prepared by the Postal Inspection Service in collaboration with its working partners.

In 2003, the Postal Inspection Service decided to broaden the scope of the Credit Card Mail Security meetings to include presentations on money laundering, Internet fraud, and bank fraud schemes. As the focus has expanded, the name of our working group has changed to the Financial Industry Mail Security Initiative (FIMSI). The initiative has decided to capture many of the best practices

developed over the years and share them with industry and law enforcement in the form of a report that will be published this year.

To manage the vast data associated with these crimes, the Postal Inspection Service has developed a new financial crimes database. This computer application compiles a myriad of intelligence data relating to financial crimes, and provides Postal Inspectors with information that assists in identifying trends, criminal hotspots, and the scope of identity theft activity. Information for this database is provided by credit card issuers, other financial institutions, mail order companies, Postal Inspection Service investigations, and the victims themselves.

### **Task Force Efforts**

In addition to partnering with members of the financial and mailing industry, task force efforts by law enforcement have been a successful approach to the identity theft issue. Postal Inspectors are active participants on financial crimes task forces throughout the nation. In Pittsburgh, Pennsylvania, the Postal Inspection Service leads the Financial Crimes Task Force of Southwestern Pennsylvania. This task force began operation on January 17, 1995, and is housed at the Pittsburgh office of the Postal Inspection Service. Originally, this task force was formed to target major credit card fraud in the Pittsburgh area. However, with the increased number of instances of identity theft spreading rapidly throughout America, this taskforce has directed most of its resources toward identity theft investigations.

One of the recent cases involved actor Will Smith as a victim of identity theft. When Smith played Agent J in the movie Men in Black that was showbiz. But when convicted felon Carlos Lomax impersonated actor Will Smith, that was identity theft. Will Smith never knew his identity had been stolen until he attempted to purchase a new home and found his credit had been compromised. Postal Inspectors and the Financial Crimes Task Force of Southwestern Pennsylvania arrested Lomax for identity theft, and Lomax was sentenced to serve 37 months in jail and pay \$64,000 in restitution.

The Minnesota Financial Crimes Task Force, which includes Postal Inspectors, Secret Service agents, and local law enforcement officers, last year arrested a Nigerian national for a \$1 million account-takeover scheme. Postal Inspectors executed a federal search warrant at the suspect's residence and recovered approximately \$16,000 in cash, three vehicles, artwork, electronics equipment, and merchandise derived from the scheme. An investigation revealed the man used bank employees to identify high-dollar, dormant accounts with balances of \$100,000 or greater for his scheme, and shipped the fraudulently obtained merchandise to his home in Nigeria.

### **Public Awareness and Education Efforts**

Over 2,000 of our 6,000 mail theft arrests last year involved identity theft -- and it's getting worse. But arrests are not the only solution. That is why the Postal



Inspection Service addresses the identity theft issue on two levels -- aggressive investigative efforts and creating prevention and awareness programs.

While the Postal Inspection Service works hard to identify and prosecute identity crimes, we also recognize our ability to lessen the impact of this crime upon the public through various prevention campaigns. Postal Inspection Service efforts to prevent identity theft target the public and business communities to educate them about these schemes, and the problems associated with them. These efforts have included the publication of a brochure titled, *Identity Theft, Safeguard Your Personal Information*, and the March 2000 release of the Showtime movie, *The Inspectors 2*, based on Postal Inspection Service files relating to identity theft investigations.

In an effort to educate consumers about this fast-growing crime, the Postal Inspection Service created an informational video titled *Identity Theft: The Game of the Name*. Also, the Postal Inspection Service and the Postal Service's Consumer Advocate Office partnered during this year's National Consumer Protection Week, from February 3 through 8. The week's theme was "Identity theft, the No.1 consumer fraud in the nation."

In 1999, Postal Inspectors along with partner organizations undertook Project kNOw Fraud, which was the largest consumer awareness campaign undertaken in this country. Through a mailing to 123 million addresses we warned the public of the dangers of telemarketing fraud. The successful campaign was followed up with the National Fraud Against Seniors Awareness Week in August of 2002. In September of this year Postal Inspectors will be unveiling another national awareness campaign. This year's topic is identity theft.

Actor Jerry Orbach, who also was a victim of identity theft, will be the campaign's spokesman. This awareness campaign features a two-pronged approach, providing prevention and awareness information to consumers and addressing businesses on the need to safeguard their files and databases of customers' personal information. The campaign will include:

- A house-to-house mailing to residences in ten states identified by the FTC as reporting the most identity theft complaints. The ten states are California, New York, Texas, Florida, Illinois, Pennsylvania, Georgia, Michigan, New Jersey, and Arkansas. The mailing will be made the first of September in conjunction with a planned press conference.
- Distribution of an updated brochure on identity theft. The brochure will be distributed in connection with identity theft presentations made by Postal Inspectors to consumer groups.

- Production and release of a Public Service Announcement (PSA) featuring actor Jerry Orbach. This thirty-second PSA will be released in September in conjunction with a press conference.
- An identity theft insert outlining prevention tips that will be included with monthly financial industry statements and with all Stamps by Mail orders placed during the months of September, October, and November.
- Production of an identity theft poster that includes prevention tips that will be displayed in all Postal Service retail lobbies, numerous credit unions, financial institutions, and police departments in September.
- Production of an identity theft informational video and articles on identity theft prevention for publication in internal and external publications as well as running newspaper ads in the same ten states that have been identified as reporting the most complaints.

The Mullen agency of Pittsburgh has provided support for this campaign on a pro bono basis. But what really makes this campaign unique is the funding source. We've all heard the saying, "crime doesn't pay." In the case of this awareness campaign, it does pay. This campaign is being funded through fines and forfeitures paid by criminals in a past fraud case.

### **Prevention Tips**

In numerous formats, including our website at [www.usps.com/postalinspectors](http://www.usps.com/postalinspectors), we provide the following recommendations to the public:

- Deposit your outgoing mail in a blue Postal Service collection box and promptly remove mail from your mailbox after delivery.
- Shred unneeded documents that contain personal information before discarding them.
- Order credit reports *every year* from each of the three major credit reporting agencies and thoroughly review them for accuracy.
- *Never* give personal or financial information over the telephone or the Internet unless *you* initiated the contact and trust them.
- Report lost or stolen credit cards immediately.
- If you applied for a credit card and didn't receive it when expected, call the financial institution.
- Sign new credit cards immediately--before someone else does.

- Memorize your Social Security number and passwords. Don't use your date of birth as your password and don't record passwords on papers you carry with you.
- Never leave transaction receipts at ATM machines, on counters at financial institutions, or at gasoline pumps.
- Don't carry your Social Security card or birth certificate; leave them in a secure location.
- Don't disclose credit card or other financial account numbers on a Web site *unless* the site offers a secure transaction.
- Closely monitor the expiration dates on your credit cards and contact the issuer if you don't receive a replacement prior to the expiration date.
- Beware of mail or telephone solicitations that offer prizes or awards--especially if the offer asks you for personal information or financial account numbers.
- Match your credit card receipts against your monthly bills and check your monthly financial statements for accuracy.
- Watch for your monthly financial statements and bills. If you don't get them when expected, contact the sender.

For victims of identity theft, we recommend the following initial steps to begin the long and arduous task of responding to the crime:

1. If the crime involved the U.S. Mail, contact your nearest U.S. Postal Inspection Service office and report it.
2. Call the fraud units of the three major credit bureaus and request a "fraud alert" be placed on your credit file. Check your monthly financial statements for accuracy.
3. Order copies of your credit report from the credit bureaus to check whether any fraudulent accounts were opened without your knowledge or consent.
4. Contact your banks and creditors, by phone and in writing, and report the crime. You may be advised to close some or all of your accounts. At the least, change your PIN codes and passwords immediately.
5. Record the names and phone numbers of people with whom you discussed your case and retain all original reports and supporting documents. Keeping accurate and complete records are a big step toward helping you resolve your problem.

6. Contact your financial institutions and request they flag your accounts. Instruct them to contact you immediately if there is unusual activity on your accounts.
7. File your complaint online with the Federal Trade Commission, or call their Identity Theft Hotline at 1-877-IDTHEFT. The FTC has counselors to assist identity theft victims with resolving financial and other problems that can result from this crime.

Educating the public and working to reduce the opportunities where the U.S. Postal Service can be used for illegal purposes are crucial elements in our fight against identity theft crimes. As always, we will do our part to remove criminals from society. We appreciate your recognition of the importance of this issue.