Statement of Lawrence Maxwell, Assistant Chief Inspector

United States Postal Inspection Service

Before the

U.S. Senate Special Committee on Aging

Hearing: "*Internet Fraud Hits Seniors: As Seniors Venture into the Web, the Financial Predators Lurk and Take Aim*

March 23, 2004

Mr. Chairman and members of the committee: thank you for holding this hearing on the topic of Internet fraud and seniors. I appreciate the opportunity to discuss the issue, and the role of the United States Postal Inspection Service in combating it.

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 1,990 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. Approximately 300 Postal Inspectors specialize in mail fraud investigations, including investigations of schemes that use the Internet to victimize the elderly.

Last year, Postal Inspectors investigated 3,150 fraud cases and our analysts prepared nearly 80,000 letters in response to mail fraud complaints. In 2003 Postal Inspectors arrested 1,453 mail fraud offenders, and 1,387 were convicted. As a result of these investigations, more than $36 million was forfeited by defendants, and prosecutions resulted in more than $2 billion in court-ordered and voluntary restitution.

History of the Mail Fraud Statute and Its Use

For more than 150 years, Postal Inspectors have pursued criminals who use the mail to defraud the unwary. Our experience with fraud investigations has encompassed countless variations of swindles from the most simple of schemes to highly complex, international frauds. A review of our many years of fraud investigations lends credence to the saying "The more things change, the more they stay the same."

In the 1800's, common frauds included failure-to-provide schemes, confidence swindles, and investment scams. The failure-to-provide schemes often involved mail order products that were never provided, or intentional misrepresentation of the goods. Confidence swindles ran the gamut of operators' imaginations that spawned inheritance schemes, offers of riches in counterfeit currency, lotteries, and a variety of frauds that appealed to basic human greed. Investment schemes included numerous variations of shady real estate offers, phony mining companies, new wonder drugs, and other grand business ventures.

Victims of early mail frauds were lured with mass advertisements, telegrams, or individual letters. Postal Inspectors and many others went to great lengths to educate the public to be wary of offers that looked too good to be true. Postal Inspectors also successfully fought these scams with basic investigative methods—the most common of which simply involved following the victims' money to the operator of the fraud.

For most of the 1800s, Postal Inspectors had few opportunities to seek prosecution for the criminals they identified operating fraudulent schemes. In response, in 1872 Congress enacted legislation relating to the Post Office

Department and the use of the mail to conduct certain fraudulent enterprises. The newly enacted law was used primarily against schemes involving the sale of worthless securities and prize contests sent through the mail. By 1896, the statute was expanded to include mailed advertisements that misrepresented the expected investment return on bonds available for purchase. As the 19th century drew to a close, the mail fraud statute was widely recognized as the weapon of choice in combating the fraud schemes of the day.

In Boston in 1919, Charles Ponzi, perhaps the most famous con artist of all time, developed what would infamously be known as a "Ponzi scheme." Simply put, the scheme works by robbing Peter to pay Paul. To lure investors, Ponzi claimed he would buy International Postal Reply Coupons from foreign countries and then redeem the coupons in this country at a substantial profit due to differences in exchange rates. Ponzi gave personal notes as security for investors' money and guaranteed a 50 to 200 percent return in 45 to 60 days. Ponzi promised that investors would make millions, and the lure of quick fortunes caused thousands to invest their money. Ponzi never bought the coupons, but by paying initial investors with money he got from new investors, he created an investing frenzy. In just seven months, more than 30,000 people paid him more than $9 million.

Ponzi was arrested by Post Office Inspectors and charged by both the District Attorney's Office and the United States Attorney's Office. He paid back some money, but then fled with several million dollars. He was caught, sent to prison and eventually deported to Italy. This didn't stop Ponzi, however. Years later, he convinced Italian dictator Benito Mussolini to give him a position in the Italian Treasury. True to form, Ponzi cleaned out a large sum and fled to South America, where he died in 1949.

From 1920 to 1940, Post Office Inspectors were active in numerous investigations that would have a lasting impact on the history of fraud. The Roaring Twenties ushered in what might be termed the Golden Age of fraud with such legendary con men as Charles Ponzi, Joseph Weil, Oscar Hartzell and others, challenging Post Office Inspectors and the mail fraud statute.

In 1927, the Bureau of the Chief Post Office Inspector formed a special unit to investigate medical fraud cases that were proliferating throughout the country. This centralized unit of specially trained Inspectors was tasked with investigating quackery cases and compiling evidence to support criminal or civil prosecutions against the promoters. Common medical frauds included alleged cures for cancer, arthritis and rheumatism, as well as worthless potions, beauty and diet products, rejuvenators and sexual devices.

In the years after World War II, work-at-home schemes conducted through the mail became more commonplace, including everything from mushroom raising, chinchilla breeding, and bead stringing to plastic laminating, artificial flower making and envelope stuffing. Postal Inspectors found one operator who was

simultaneously running 44 related companies promoting work-at-home schemes.

By the late 1960s, the mail fraud statute became a key weapon in the war against organized crime. Organized crime strike forces in U.S. cities brought successful prosecutions against mobsters. Postal Inspectors joined these strike forces and participated in successful multi-agency investigations and prosecutions. Through the Organized Crime Control Act of 1970, mail fraud was considered a racketeering activity and a RICO (Racketeering Influenced and Corrupt Organizations) predicate.

The language of the mail fraud statute remained unchanged for 100 years. It wasn't until 1994 that Congress expanded and enhanced the statute as part of the Violent Crime Control and Law Enforcement Act, inserting new language into Section 1341 that reads "or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier." Con artists who try to circumvent the mail by using private interstate couriers are no longer exempt from the law, as the 1994 Crime Bill amended the mail fraud statute to include them. The mail fraud statute can now be used for items sent through the U.S. Mail, as well as FedEx, UPS or other interstate carriers and couriers.

Working closely with the Senate Permanent Subcommittee on Investigations, Postal Inspectors helped craft legislation that addresses fraudulent sweepstakes and other deceptive mailings. As a result, the Deceptive Mail Prevention and Enforcement Act was passed and became law in April of 2000. The law protects consumers, especially seniors, against deceptive mailings and sweepstakes practices by:
• establishing standards for sweepstakes mailings, skill contests and facsimile checks,
• restricting government look-alike documents, and
• creating a uniform notification system allowing individuals to remove their names and addresses from all major sweepstakes mailing lists at one time.

Mailings must disclose in clear and prominent language that no purchase is necessary to enter a sweepstakes and that a purchase will not improve consumers' chances of winning a prize. The law also creates strong financial penalties for companies that do not disclose all terms and conditions of a contest.

Throughout the 1900s, Postal Inspectors investigated a myriad of complex and noteworthy cases ranging from the swindles of the past like the Ponzi scheme to new twists on old scams, from investments to health care, many of which had evolved to incorporate telephone communications, radio, and/or television pitches. Telemarketing "boiler rooms" gave rise to some spectacular frauds. The fraudsters had some new tools to use against their victims, and they modified the many variations of existing frauds to best exploit the new technology. Despite the many new variations, the underlying basis continued to primarily be failure-to-

provide schemes, confidence swindles, and investment scams, and the premier fraud-fighting tool continued to be the mail fraud statute.

The Electronic Age

The incredible rise in Internet use has provided another new avenue for swindlers to pitch their frauds. Even more anonymous than mail, telephone, or television, this powerful medium has allowed criminals to pursue even more victims, and also has further broken the barriers of national borders, time zones, and investigative jurisdictions. A single operator working on a computer anywhere in the world can now instantly reach millions of potential victims everywhere the Internet reaches, and the victims' money can be moved electronically from credit cards or bank accounts directly to the fraudster.

The basic elements of the fraud have changed little. However, the evolution of fraudulent schemes to an electronic world has created new challenges for law enforcement officers that investigate the crimes. Following the victims' money can be an extremely complicated effort involving electronic funds, anonymous communications, complex network infrastructures, and multiple countries. The old techniques, while still very effective, require new tools, knowledge, and international logistics.

Internet Frauds and Elderly Victims

Older citizens, the physically challenged, and "shut-ins" conveniently receive many of their purchases by mail. Sadly, that makes them easy prey for mail fraud operators. Legitimate retailers have greatly increased their online presence, and older citizens have followed. Once online, they naturally expand their use of Internet resources and e-mail, and this increases the likelihood that they will encounter fraudulent schemes.

Americans receive millions, perhaps billions, of unsolicited e-mails each year trying to sell a variety of products, with older citizens often the target. By definition, Internet fraud involves the use of the electronic communication. But e-mails, online auctions, or fraudulent websites often involve the use of the U.S. Mail. Since many fraudulent transactions require the exchange of money or goods, it is difficult to completely avoid the use of the mail. When the mail is involved in any way, the crimes fall within the purview of the Postal Inspection Service.

An important investigative method includes the compilation of statistics relating to current trends. The Postal Inspection Service maintains a database of reported frauds and details of our investigations. This database provides information that can be useful in analyzing how fraudulent schemes affect our society.

In 2002, the Postal Inspection Service received 13,034 complaints regarding

allegations of fraud involving the Internet. In 2003, the number rose to 18,534. In the first five months of our current fiscal year, the number of Internet related fraud complaints has increased by nine percent from the 2003 figures.

The numbers of elderly victims also increased from 2002. In that year, we received 2,017 complaints from victims over the age of 55. In 2003, we received 8,397 complaints from seniors. We also compiled records regarding the types of complaints received from seniors. In the last three years, the most commonly reported fraud was associated with failure-to-provide transactions. The primary source of these complaints stems from the growing numbers of older Americans participating in Internet auctions. As more seniors use Internet auctions to purchase merchandise, they become a larger share of victims for the operators of fraudulent auctions.

In one failure-to-provide investigation that has been reported as the largest Internet auction fraud in history, Postal Inspectors arrested a 25-year-old Connecticut woman who used the eBay auction service to sell $800,000 in computers to some 300 buyers. But she didn't provide computers to many of the victims. Each time eBay received customer complaints and suspended her from conducting business on its site, she would change to another identity, many of which belonged to her employees or friends. When irate buyers confronted her by telephone or e-mail, she gave them a series of false explanations, excuses, and promises of imminent refunds. However, she was unable to refund all of the money she had received, since she had spent much of it on living expenses and to start her own advertising business, which ultimately failed. While not specifically targeting seniors, we encountered several elderly people who had been victimized in this case. She was prosecuted for the fraud, and sentenced to serve 58 months in federal prison.

The Postal Inspection Service is currently seeking prosecution in another failure-to-provide scam involving eBay auctions. This past October, a 16-year-old suspect obtained an Illinois state-issued identification card using a false identity. He then posted eBay auctions for merchandise he did not have, and requested payments be sent by check or money order to a post office box obtained using the fake ID card. He did not provide any merchandise for the payments he received.

Surprisingly, this fraud was not his first. In 2002, when he was only 15 years old, he conducted a similar scheme. In the first case, his parents agreed to reimburse the victims, and he avoided prosecution. We have identified 40 victims, several of whom are elderly, who typically mailed several hundred dollars each for the non-existent merchandise. One elderly victim did not even have direct Internet access, and had asked a co-worker to bid for her in an auction of two laptop computers. The intended auction fraud amount in this scheme was approximately $26,000.

There are also some new variations of old frauds that are unique to the Internet. Schemes known as “spoofing” and “phishing” are techniques we now encounter in some investigations. Postal Inspectors recently participated in an investigation that highlights the use of phishing in a new version of an old fraud. In this case, operators in the Ukraine generated thousands of e-mails sent to targets in the United States. The e-mails were designed to mimic communications from legitimate online businesses, including Citibank, eBay, and PayPal. However, the e-mails requested personal identifying information, such as account numbers, screen names, and passwords.

The illegally-obtained account information was used to purchase goods online, or funds were transferred electronically. In order to execute the fraud, the suspects recruited individuals in the United States to receive merchandise and money on their behalf. The recruited individuals were directed to deposit the money into their accounts and forward the money to other accounts in the U.S. and overseas to be laundered. Where stolen merchandise was involved, the recruited individuals were directed to forward it on to individuals in Eastern Europe. The U.S. Mail and other private express carriers were used extensively in the execution of this scheme.

Four Ukraine police officers were arrested for their involvement in the phishing fraud, and their computers were searched for evidence. Based on evidence recovered from the search and discussions with victim companies, the losses to U.S. account holders in this case is estimated at $4.2 million.

Another twist on Internet auction frauds involves counterfeit checks. Since November 2003, the Postal Inspection Service has teamed with British Customs and Excise to specifically target Nigerian-based Internet auction frauds. In these cases, counterfeit checks are mailed to individuals in America who have sold an expensive item, including automobiles, through an Internet auction. Often, the checks are sent to a bank manager to deposit directly into the victim's account, adding to the appearance of a legitimate mailing. However, in this scam the counterfeit check exceeds the amount requested by the seller, often by thousands of dollars, and the seller is instructed to wire the excess funds to Europe or Africa. Several weeks later, the seller learns the check is counterfeit.

In our task force response to this type of scam, packages of counterfeit checks from Africa and Europe are intercepted in a combined effort with the United Kingdom National Criminal Intelligence Service, and British Customs & Excise. We often find packages containing forty to fifty checks with combined values of several hundred thousand dollars. Typically, the individual checks are already in pre-addressed envelopes ready to be placed in the U.S. Mail for delivery to unsuspecting victims. In addition to seizing the counterfeit checks, we also aggressively pursue the criminals involved. Our efforts to prevent these frauds have been quite successful, in part due to our established international partnerships to combat credit card fraud.

Other examples of Internet-based mail fraud against consumers investigated by Postal Inspectors are illegal contest and sweepstakes schemes, chain letters, travel and vacation fraud, merchandise misrepresentations, phony billing scams, and misleading investment opportunities. In addition, there are work-at-home schemes, rebate fraud, and foreign lottery fraud – all using the Internet and electronic mail to reach potential victims. As older people continue to expand their use of electronic communications, they will be increasingly subject to these frauds, even if the operators do not specifically target the elderly. The problem is compounded by operators who sell the names and addresses of their victims to other criminal elements, resulting in the repeated victimization of many elderly citizens.

Tactics Used by Fraudulent Operators

Many senior citizens are vulnerable to being victims of Internet frauds that seek much more than the cost of a one-time auction sale. Many telemarketing frauds also use the Internet to locate and identify elderly victims. Fraudsters recognize that many seniors are widowed and more likely to feel isolated. For the lonely, a telephone call from anyone is greeted with open arms. When they obtain telephone contact information for their potential victims, the fraud operators start calling. Experienced con artists understand elderly citizens' vulnerabilities and know what psychological buttons to push when they have them on the telephone.

In searches of telemarketers' places of business, we have discovered the files they maintained on their victims. The files contained intimate details of the victims' health, the names of their children, vacation and travel memories, and even information on deceased spouses. Telemarketers, in particular, use this personal information when they call their victims. They mention family names, inquiring solicitously about their health, and very effectively portray themselves as being caring and knowledgeable. For the victims, these telephone calls may be their only regular contact with other people, and the victims actually value the interaction with someone willing to talk with them. Victims often even defend the fraud operators in the continued belief that they are "friends" who are trying to help them win a sweepstakes or manage investments. Some victims will even acknowledge that the fraud operator is taking advantage of them, but explain that they had no one else who showed interest in them.

"You have won" schemes target elderly victims who have previously participated in online lotteries, sweepstakes, and other prize winning opportunities. Seniors are told that they have won—however, either administrative fees, taxes, or membership fees must be paid before the prize check can be mailed. Foreign fraud operators are notorious for this type of scam. They are aggressive and fearless since they are in a different country, and they understand how difficult extradition can be to the United States. This is why the Postal Inspection Service is one of the leading agencies in the Cross-Border Fraud Investigative Initiatives

and work closely with law enforcement agencies in cooperating countries.

Another tactic utilized by con artists is to tell a senior that they have won a large cash prize and then ask them to verify their identification by providing a credit card or bank account number so they can verify they have the right winner. These operators are very persuasive, and once they obtain the personal financial information of a victim, they can clean out their accounts.

One of the most notorious scams against seniors is what is known as the "reload." When fraud operators are successful in obtaining money from a victim, they often make an attempt to gain even more. This is the reload. In a typical reload, the fraud operator contacts the victim again and builds upon the original scam by adding a new twist to it, or pitches an entirely new scam. Sweepstakes “winners” may be told that their prize winnings have increased, but that additional fees are necessary to claim the new amount. Victims of fraudulent investment schemes may be convinced to invest even more money, or to convert their original investment to another market product which is invariably worth even less than what the victims were sold before. Fraudulent operators also often network with each other. They sell each other the names of people they have successfully ripped off. The con artists refer to these lists as “mooch lists” or “sucker lists.” If a fraud operator knows a particular senior has fallen victim to several scams, they sometimes contact the elderly victim and pose as an attorney or law enforcement officer and claim that they have recovered the victim’s money and it is either in a state fund or being held by the courts. The operator will then request an administrative or bonding fee to release the funds, and in doing so steal from the victim again.

Impact on Victims

Illegal fraud schemes continue to target senior citizens who are often the most vulnerable and trusting. Many senior citizens have been robbed of their hard-earned life savings and frequently pay an emotional cost, losing not only their money, but also their self-respect and dignity. Postal Inspectors have interviewed victims who claimed they could not remember sending anything to the operators, or, out of embarrassment, minimized the level of victimization they experienced.

Interagency and Industry Cooperation

To increase efficiency in investigating suspected mail fraud, Postal Inspectors lead or participate in several law enforcement and consumer group initiatives aimed at safeguarding the public’s confidence in the U.S. Mail, and protecting consumers. Listed below are some of our major cooperative efforts.

Health Care Fraud Working Group
Chaired by the Department of Justice (DOJ) Fraud Section, this interagency group seeks to share investigative strategies, prevention and training programs

and develop best practices in fighting health care fraud affecting those dependent on health care, mostly seniors, and the American government which bears much of the costs. Members include DOJ, the FBI, Health and Human Services Office of the Inspector General, state attorneys general offices, various health care groups and the Postal Inspection Service. The Postal Inspection Service is also an active law enforcement member of the National Health Care Anti-Fraud Association (NHCAA).

Telemarketing and Internet Fraud
The Telemarketing and Internet Fraud Working Group is chaired by DOJ and as the name implies, focuses on the large problem of telemarketing and the dramatically increasing use of the Internet in fraud schemes. The former impacts the elderly significantly. This working group was the one which first brought attention to the cross-border problem of telemarketers operating in Canada and focusing on U.S. victims to evade prosecution. U.S. law enforcement was frustrated in its attempts to investigate and apprehend these operators in Canada, due to national sovereignty issues. It served as a catalyst in the development of the Cross-Border Crime Forum (see below). Members of this group include DOJ, the FBI, Federal Trade Commission, Secret Service, state attorneys general offices, and the Postal Inspection Service.

Corporate Fraud Task Force
Created in the wake of the Enron scandal to address the corporate criminal mismanagement, the corporate fraud task force was initiated by a Presidential Directive. Although the term “corporate fraud” implies a business fraud, the vast majority of the victims are the consumer investors who trusted the integrity of the firm. Many seniors have lost their life savings through this wave of corporate greed. The members of the group include several United States Attorneys in districts where the problem appeared, the Treasury Department, the Labor Department, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), Federal Energy Regulatory Commission (FERC), Federal Communications Commission (FCC) and the Postal Inspection Service.

Council on White Collar Crime
Chaired by the Attorney General and his staff, this working group meets once a year and includes all the major agencies involved in combating white collar crimes, both civilly and criminally.

Securities and Commodities
Chaired by DOJ to focus on fraud in the stock market, its members include the Postal Inspection Service, the FBI, the SEC, the IRS, the Secret Service and various U. S. Attorneys.

Cross-Border Crime Forum
Established by another Presidential Directive, the Cross-Border Crime Forum

meets once a year to address problems and solutions to cross-border crimes. Members include DOJ, the FBI, FTC, Customs, the Postal Inspection Service and our Canadian counterparts.

Consumer Education and Fraud Prevention Initiatives

Criminal prosecution is an important element in our fraud program, but it is not the only tool. Arrests are not the only solution. The Postal Inspection Service works to protect consumers by educating them about current fraud schemes. At some point, most consumers will be the target of a fraudulent scheme, but they do not have to be victims. For years, Postal Inspectors have led fraud prevention projects and participated with consumer protection agencies and other groups to help citizens protect themselves before they become victims of fraud.

"Operation Cyber Sweep"
This was a joint law enforcement initiative with the FBI and other law enforcement agencies, announced at a press conference on November 20, 2003. The Chief Postal Inspector participated in the press conference along with Attorney General John Ashcroft and others. The sweep resulted in the arrests of 125 suspects in a crackdown on Internet crimes ranging from hacking to fraud to selling stolen goods. The sweep involved police from Ghana to Southern California and uncovered 125,000 victims who had lost more than $100 million. Many suspects were accused of selling stolen or nonexistent goods online. Suspects also stole classified files from government computers, hacked into business computers to steal customers' credit-card numbers, disabled computers running child-abuse hotlines, and sold counterfeit software or computer-memory chips.

Project kNOw Fraud
Responding to the proliferation of telemarketing fraud cases, the Postal Inspection Service led an interagency group of law enforcement and consumer organizations in what was named Project kNOw Fraud, one of the most ambitious fraud prevention initiatives ever undertaken. In 1999, Project kNOw Fraud sent a postcard to every household in America—more than 123 million addresses. The card contained valuable telemarketing fraud prevention tips. The project included a Web site and toll-free number to call for additional information or to report a fraud. In addition, a telemarketing fraud prevention video was produced and delivered to more than 15,000 public libraries. Funding to print, address and prepare the mailing for distribution came from money seized by the Postal Inspection Service in a telemarketing fraud case.

National Fraud Against Senior Citizens Awareness Week
People 60 years of age and older accounted for 26 percent of telemarketing fraud victims in 2001, according to the Alliance Against Fraud in Telemarketing and Electronic Commerce. Seniors, however, showed a much higher representation in specific categories—especially prize and sweepstakes fraud—

where they accounted for 60 percent of the victims. In a hearing before the Senate Permanent Subcommittee on Investigations in June 2001, Postal Inspection Service representatives and the Pittsburgh Senior Action Coalition discussed the idea of having the Inspection Service and the Coalition initiate a national campaign with other agencies to raise the awareness of older citizens about illegal telemarketing and mail fraud schemes.

In support of the effort, the Senate passed a resolution, introduced by Senators Carl Levin and Susan Collins, designating the week of August 25, 2002, as "National Fraud Against Senior Citizens Awareness Week."

On August 26, 2002, the Chief Postal Inspector joined forces with Postmaster General John E. Potter, Federal Trade Commission Chairman Timothy J. Muris, Assistant Attorney General Michael Chertoff, and representatives of the Royal Canadian Mounted Police to announce the campaign kick-off. Popular actress Betty White, who fits the age range of the targeted group, signed on as spokesperson for the campaign. A total of 51 press events were held in cities nationwide.

Nationally, a multimedia campaign encompassed a wide range of activities: fraud awareness posters were created and posted at more than 38,000 Post Offices across the country; brochures were inserted in Postal Service mailings of stamps and philatelic materials; half-page ads were placed in 40 major metropolitan newspapers; public service announcements featuring Betty White were broadcast on television and radio stations; and fraud awareness flyers were mailed to roughly three million households of seniors and their families.

The Postal Inspection Service's Web site, www.usps.com/postalinspectors, promoted the campaign and offered seniors tips on how to protect themselves from mail and telemarketing fraud. Hundreds of consumer-oriented organizations with Web sites catering to older citizens added links from their sites to the Postal Inspection Service site.

An immediate success of the campaign was declared when, during its first week, a woman in her 80s went to a small Post Office near Pittsburgh, Pennsylvania, to mail a $2,200 cashier's check to Canada, telling the postmaster she needed the money right away because her husband had won $162,000 in a Canadian sweepstakes. She had to mail the check to pay for taxes on the winnings before she could receive the prize money. The postmaster, educated by the Postal Inspection Service's campaign, told her "Don't mail him anything. It's a scam." And it was. The venture was being investigated by Postal Inspectors and our Canadian counterparts.

National Consumer Protection Week
In 1999 and 2000, the Postal Inspection Service and the Postal Service Consumer Advocate's Office joined the AARP, Consumer Federation of America,

Department of Justice, Federal Trade Commission, National Association of Consumer Agency Administrators and National Association of Attorneys General to launch National Consumer Protection Week (NCPW). The purpose of NCPW is to educate consumers about various types of mail fraud, including identity theft.

In 2001, the NCPW theme was “If it’s too good to be true, it probably is.” The campaign focused on the technological advances that have provided new avenues for scams that were once perpetuated solely through the use of the mail. The theme for 2002 was “Deceptive Mailings – Don’t Be Duped.” An educational video news release was issued featuring Senators Susan Collins and Carl Levin speaking on the Deceptive Mail Prevention and Enforcement Act. In February 2003, NCPW focused on identity theft, which is currently the fastest growing crime.

Operation: Identity Crisis
In September 2003, the Postal Inspection Service, in conjunction with the U.S. Postal Service, the Federal Trade Commission, the U.S. Secret Service, and various other government agencies and private companies unveiled a national consumer awareness campaign. Known as “Operation: Identity Crisis,” the campaign focuses on the ease with which identity theft occurs unless consumers take steps to prevent it. This crime affects all age groups, including older Americans. The percentage of seniors as a victim group rose from 17 percent to 23 percent as reported by the FTC in 2003.The campaign also provides prevention tips to businesses to help them protect consumer data and ensure privacy.

The national information campaign features newspaper ads appearing in 17 newspapers in markets with the highest number of identity theft complaints (Arkansas, California, Florida, Georgia, Illinois, Michigan, New Jersey, New York, Pennsylvania, and Texas) and a three million piece mailing to residents in the above-mentioned states. Jerry Orbach of television’s Law & Order, as the national spokesman, appears in Public Service Announcements. Also as part of the campaign, the Postal Inspection Service produced a new consumer video on identity theft entitled “Identity Crisis,” and revised a Postal Inspection Service brochure on identity theft.

Crime Doesn’t Pay…or Does It? The Consumer Fraud Fund

We recognize that the success of the fraudulent operator depends heavily upon the victim’s participation. Fraud is a crime that can be reduced or prevented by educating the general public and specific groups, like the elderly. Accordingly, the Postal Inspection Service established the Consumer Fraud Fund to augment fraud prevention programs. The fund was created with monies received from criminal fines and forfeitures in cases where victims could not be identified. The consumer protection programs that will be financed using the fund entail a

series of fraud prevention programs designed to educate the American public and to create consumer awareness of the various fraud schemes being perpetrated, including many which are aimed at the elderly population.

Enhanced Enforcement

To make the most effective use of the Deceptive Mail Prevention and Enforcement Act of 1999 and protect consumers, the Postal Inspection Service established a Deceptive Mail Enforcement Team, composed of Postal Inspectors, Inspector Attorneys and Inspection Service fraud analysts. The team reviews complaints related to promotional mailings to assess their compliance with the Act and ensure swift, investigative attention as appropriate.

Other Enforcement Strategies

In those instances where the crime does not meet federal prosecutorial guidelines, Postal Inspectors bring their cases to local prosecutors or seek alternative solutions. Regrettably, most frauds target those who can least afford it—the elderly, the poor, the disadvantaged, or the ill. These frauds most often result in relatively small monetary loss and are not always prosecutable under federal guidelines. Although the loss is significant to the victim, it is often not significant enough to support a federal criminal action.

In these cases, we seek alternative resolution whenever the crime is certain, but lacks criminal prosecutive appeal. Alternative resolutions consist of civil or administrative action. In instances where the criminal activity does not meet federal or state prosecutive guidelines, yet the scam affects a large number of consumers, often the most disadvantaged, Postal Inspectors take quick action to withhold mail or to encourage the promoter to voluntarily discontinue the fraud. Over the past decade, more than 5,500 envelope stuffing, chain letter and coupon fraud scams have been halted in this manner. We have achieved similar success in combating illegal foreign lottery mail. Since 1994, over 10 million envelopes containing foreign lottery material have been destroyed.

Withholding Mail Order
A Withholding Mail Order (Title 39, USC 3003) enables the Postal Service to withhold an addressee's mail if they are using a false or assumed name to conduct or assist with activity that violates lottery, mail fraud or use of a fictitious name or address statutes.

Temporary Restraining Orders and False Representation Orders
The Postal Service has unique remedies for civil/administrative relief under the postal false representation and lottery statutes, Sections 3005 and 3007 of Title 39. Temporary Restraining Orders (TROs) and False Representation Orders (FROs) enable Postal Inspectors to stop mailed-in responses (most of which contain checks) before they reach the operator of a fraud scheme. An immediate

stop of mail requires a TRO, which is sought from a U.S. District Court with approval by and assistance from the United States Attorney's Office. If a TRO is issued, the mail is detained pending completion of administrative proceedings. FROs are issued by a Postal Service Judicial Officer. If issued, mail sent to the promoters will be returned to its senders, thereby preventing victim losses.

FROs are often used to combat illegal lotteries, both foreign and domestic. Lottery promotions usually involve the purchase of a share in a foreign lottery pool and promise large winnings for little effort. They often target senior citizens who are most vulnerable to such scams. Such promotions are usually conducted from a foreign country. Those who pay money to enter a pool that plays numbers in an overseas lottery usually see no return, even if one of the pool's numbers wins, because participants are usually not made aware of what numbers are played or what numbers win. If a pool number does win, and a payout is made to participants in the pool, it is often in an amount disproportionate to a participant's share of the pool, but a participant has no way of knowing that.

Reporting Fraud Complaints

Each year the Postal Inspection Service responds to thousands of consumer fraud complaints received through our toll-free mail fraud hot line, online complaint system, or by mail. In addition, we receive numerous complaint referrals from federal, state and local law enforcement agencies, prosecutors, and industry and consumer groups. Nearly all of these complaints question the legitimacy of promotional offers they received in the mail. Postal Inspectors urge consumers to report incidents of potential mail fraud. Information that is collected by complainants is input to the Postal Inspection Service's Fraud Complaint System, which helps identify violators of the Mail Fraud or False Representation Statutes.

Civil Asset Forfeiture Reform Act

The Civil Asset Forfeiture Reform Act (CAFRA) of 2000 was of great help to Postal Inspectors resolving fraud cases. Prior to CAFRA, when the best or the only way to seize proceeds of a fraud was forfeiture, the requirements of forfeiture were such that it was very difficult to provide victim restitution. Moreover, it was only possible to pursue forfeiture in mail fraud cases when money laundering could be proven. CAFRA changed all of that. Now forfeiture of assets in mail fraud cases can be accomplished by showing the property is a proceed of the crime. Further, restitution to identified victims is through a much more efficient and simplified process.

Frequently Asked Questions About Mail Fraud and Prevention Tips

Below are frequently asked questions about mail fraud schemes, as well as tips and suggestions to assist consumers in identifying a potential fraud.

Which schemes generate the most complaints?

1. Contest and sweepstakes fraud. A consumer is told he or she is a guaranteed prize winner, but the “free” prize could end up costing hundreds of dollars, and often the victim never receives a thing
2. Chain letters. These usually require the recipient to send money to others on a list. The letter promises fantastic earnings to participants if the chain is continued. They fail to tell participants it is mathematically impossible for every person to benefit.
3. Foreign lotteries. Any lottery involving a foreign country and conducted through the mail is illegal; they may also be fraudulent. You may not even be entered to play.
4. Travel scams. Recipients are promised a dream vacation, which becomes a nightmare. Travel arrangements are either unavailable when the traveler wants to go, or transportation and lodging are paid for in advance, but not booked by the travel agent, who pockets the money.
5. Work-at-home schemes promise work stuffing envelopes or assembling products. The only real work is selling the program to dupe others into falling for the scheme.
6. Investments. Enticing pitches promise low-risks with high returns in exotic minerals, strategic metals, and rare gemstones, ostrich ranching or other “can’t miss” offers.
7. Phony billing scams. These target businesses and professionals, using unsolicited calls or letters offering Yellow Page ads, copy machine supplies, specialty advertising items and other overpriced products. They may imply they are your regular supplier offering a special discount.
8. Internet auction fraud. Buyers place bids for items on an auction Web site. Successful bidders “win” the auction and pay via the U.S. Mail. They’re scammed when the seller doesn’t deliver the goods after receiving payment, delivers something other than the advertised item, or doesn’t disclose relevant information about the item. Inspectors investigate Internet fraud when the mail is used as part of the scam.

Other common types of mail fraud include advance-fee loans, credit repair offers, business opportunities scams, home improvement schemes and supplemental health insurance frauds, to name a few.

Are the fraudulent schemes directed at any particular group?
Sophisticated con artists target older citizens who often live alone, have sizable savings accounts and may be disarmed by convincing salespeople. Favorite schemes include sweepstakes scams, guaranteed prize promotion investments and foreign lotteries. Many seniors are victimized repeatedly through the sale of victim lists. Other operators offer to help recover victims’ previous losses—for a fee, only to scam them all over again.

How do people avoid being scammed?

A consumer's good judgment is the last line of defense against the con artist. Consumers should be skeptical of any offer that sounds too good to be true. The following questions can help consumers evaluate questionable offers:

- Do I have to pay to receive a "prize" or enter a sweepstakes?
- Do I have to provide personal or financial information?
- Am I a "guaranteed" winner or told "no risk is involved?"
- Am I pressured into responding right away?
- Do they ask for advance payment or accept cash only?

If the answer is "yes" to any of these questions, consumers should be wary. Consumers should ask that all statements about the product or service be provided in writing, and check the offer with the consumer protection agencies, the Better Business Bureau (BBB), State Attorney General, or the National Fraud Information Center, at 1-800-876-7060.

The Postal Inspection Service's Web site, www.usps.com/postalinspectors,offers more tips on postal-related crimes and allows consumers to submit a mail fraud complaint online. Fraud complaint forms are also available at every Post Office. In addition, the Postal Inspection Service offers several publications to assist consumers in preventing mail fraud.

Copies of the following publications may be obtained by calling 1-800-332-0317.

- Publication 280, Safeguard Your Personal Information
- Publication 300-A, Consumer and Business Guide to Preventing Mail Fraud
- Publication 281, Consumer Fraud by Phone or Mail, Know How to Protect Yourself

The Postal Inspection Service, partnering with other law enforcement agencies, will continue to aggressively pursue those who use the Internet and the mail to prey on our citizens. We will do our best to make sure any new versions of old frauds receive the same swift action Postal Inspectors have provided for generations, and America's trust in the mail remains firm.