AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 108–486

# INTERNET FRAUD HITS SENIORS: AS SENIORS VENTURE INTO THE WEB, THE FINANCIAL PREDATORS LURK AND TAKE AIM

## HEARING

BEFORE THE

## SPECIAL COMMITTEE ON AGING
## UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

WASHINGTON, DC

MARCH 23, 2004

**Serial No. 108–32**

Printed for the use of the Special Committee on Aging

U.S. GOVERNMENT PRINTING OFFICE

93–526 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SPECIAL COMMITTEE ON AGING

LARRY CRAIG, Idaho, *Chairman*

RICHARD SHELBY, Alabama
SUSAN COLLINS, Maine
MIKE ENZI, Wyoming
GORDON SMITH, Oregon
JAMES M. TALENT, Missouri
PETER G. FITZGERALD, Illinois
ORRIN G. HATCH, Utah
ELIZABETH DOLE, North Carolina
TED STEVENS, Alaska
RICK SANTORUM, Pennsylvania

JOHN B. BREAUX, Louisiana, *Ranking Member*
HARRY REID, Nevada
HERB KOHL, Wisconsin
JAMES M. JEFFORDS, Vermont
RUSSELL D. FEINGOLD, Wisconsin
RON WYDEN, Oregon
BLANCHE L. LINCOLN, Arkansas
EVAN BAYH, Indiana
THOMAS R. CARPER, Delaware
DEBBIE STABENOW, Michigan

LUPE WISSEL, *Staff Director*
MICHELLE EASTON, *Ranking Member Staff Director*

# CONTENTS


| | Page |
|---|---|
| Opening Statement of Senator Larry E. Craig | 1 |
| Statement of Senator Susan Collins | 2 |
| **PANEL I** | |
| Jeffrey Groover, inmate, Federal Correctional Institution, Yazoo City, MS | 3 |
| **PANEL II** | |
| Dave Nahmias, Deputy Assistant Attorney General, Criminal Division, Department of Justice, Washington, DC | 8 |
| Lawrence E. Maxwell, Assistant Chief Inspector, U.S. Postal Inspection Service, Washington, DC | 27 |
| J. Howard Beales, III, Director, Bureau of Consumer Protection, The Federal Trade Commission, Washington, DC | 47 |
| Tanya Solov, director of Securities, North American Securities Administrators Association, Chicago, IL | 70 |
| David Jevans, chairman, Anti-Phishing Working Group, Redwood City, CA | 77 |

# INTERNET FRAUD HITS SENIORS: AS SENIORS VENTURE INTO THE WEB, THE FINANCIAL PREDATORS LURK AND TAKE AIM

---

**TUESDAY, MARCH 23, 2004**

U.S. SENATE,
SPECIAL COMMITTEE ON AGING,
*Washington, DC.*

The committee met, pursuant to notice, at 10:34 a.m., in room SD–628, Dirksen Senate Office Building, Hon. Larry E. Craig (chairman of the committee) presiding.

Present: Senators Craig and Collins.

## OPENING STATEMENT OF SENATOR LARRY CRAIG, CHAIRMAN

The CHAIRMAN. Good morning, everyone. The Special Committee on Aging will be convened. The subject today, Internet Fraud Hits Seniors: As Seniors Venture into the Web, the Financial Predators Lurk and Take Aim. I would like to thank our witnesses for joining us today on an issue of growing national concern, the emerging use of the Internet to perpetuate fraud against our nation's senior citizens.

According to a recent survey, those 65 years of age and older are the fastest-growing group online, increasing their presence on the Internet by 25 percent in 2003. As seniors go online in record numbers, fraud perpetuated through the Internet is dramatically on the rise. Thousands of Internet fraud victims in 2002 were senior citizens and those numbers nearly doubled in 2003. Seniors are also targeted in disproportionate numbers by scams originating across borders and overseas.

We know that the Internet offers a vast global marketplace for consumers and businesses alike. Unfortunately, scam artists also recognize the potential of the Internet for criminal enterprises. The same scams that were once conducted by mail and phone are now easily perpetuated through the Internet, and new scams emerge every day. Criminals know that they can commit fraud online in a faster and more cost-effective way. They also know it is harder to get caught.

Therefore, to effectively fight this crime, it is critical that the State and Federal law enforcement agencies work closely together. In cases of Internet fraud committed across borders, it is important for domestic law enforcement to work effectively with their foreign counterparts. As part of this hearing, I am pleased to announce a new public awareness Initiative with Federal agency partners to

educate the senior population on the new dangers of Internet fraud. The FTC is our lead partner in this effort.

In conclusion, I also urge the law enforcement agencies represented here today to be on the alert for Internet fraud related to the new Medicare prescription drug discount card program that this committee reviewed just a few weeks ago. Although no Internet fraud reports have been reported as of yet, we must remain ever-alert to new ventures or avenues of criminal activity.

Before I introduce our first panel, let me turn to my colleague Susan Collins who, through her committee, has already done work in this area.

**STATEMENT OF SENATOR SUSAN COLLINS**

Senator COLLINS. Thank you very much, Mr. Chairman.

I am very pleased that you are holding this hearing today on such an important issue. I have long been concerned about the problem of Internet fraud, particularly those scams targeting our elderly. The Internet is a phenomenal tool of commerce and communication, but it also provides a powerful tool to those who would use it for criminal purposes.

The Permanent Subcommittee on Investigations, which I formerly chaired, held a series of hearings related to fraud and the Internet. We began the series in 1998 with a hearing on the very topic that we are addressing today, Internet scams and how they affect consumers, particularly our senior citizens.

I recall saying at the time, this was 6 years ago, that 175 countries were connected to the Internet and approximately 50 million Americans were using the Web. I thought that was astonishing at the time. Well, today, of course, that number has grown to at least 203 countries and 165 million Americans who regularly use the Internet to pay their bills, shop online, or simply to search for information or communicate with their friends and family.

There is no question that the Internet has been a boon for business. The remarkable ease and speed with which transactions can be conducted over the Internet have made the world a smaller place. Consumers have the ability to engage in a variety of commercial activities across State and even national borders, including shopping, banking, and investing, all from the comfort, privacy, and safety of their own homes. An unfortunate corollary to this ease of access, however, is that those who wish to use the Internet to defraud innocent people can also work just as easily from the privacy, comfort, and safety of their own homes, or anywhere else, for that matter. Because the Internet can be used to transfer text, pictures, music, as well as money, credit card numbers, and other personal information, the potential for criminal use of the Internet is infinite.

Corresponding to the explosive growth of the Internet, the number of consumer complaints of Internet fraud to the Federal Trade Commission continues to rise. Of the nearly 302,000 fraud complaints filed last year, more than 166,000 people reported that they had been victims of Internet-related fraud. That is more than a doubling of the number of victims in the last three years. The cost of this escalating fraud? Nearly $200 million, including $12.8 million paid out by defrauded seniors, many of whom are living on

limited incomes. Those are only the ones who actually took the time to file complaints with the FTC. The real number is undoubtedly much higher.

Seniors can be especially vulnerable to Internet fraud. Some of the very achievements that they have worked their whole lives to attain contribute to this vulnerability. Many seniors have strong credit records earned over years of faithfully paying their bills on time. This good credit is being abused by thieves who steal their credit card numbers to run up bills on their accounts, or by others who promise huge returns on an investment that never materializes.

Law enforcement officials know that almost any crime that can be committed in the real world can also be committed in the virtual world. In fact, the Internet allows criminals to target their victims more quickly, less expensively, and with much less chance of getting caught.

So again, Mr. Chairman, I salute you for undertaking this effort. I think one of the most important things we can do for our seniors is to educate them and alert them to the potential for fraud. I know that has been the focus of your efforts as chairman, and I salute you for that.

The CHAIRMAN. Senator, thank you very much for that statement. Those facts, the statistics of access to and, now, regular use of the Internet are really phenomenal and are still moving by large numbers in this country.

Now let us move to our panelists and our first panel. Our first panelist is Jeffrey Groover, a former Internet service business owner and currently an inmate of the Federal Corrections System, who will share with us his experience with Internet fraud. I must tell you, Jeffrey, I am pleased that you were willing to testify today and you were allowed to testify. I think it is important for the record that we hear first-hand from someone who has effectively used the Internet for criminal activity.

Mr. Groover, since you will be testifying as to the facts in a case that you have first-hand knowledge of, we need to take your testimony under oath. Would you please stand and raise your right hand.

Jeffrey Groover, do you solemnly swear that the testimony you are about to give before the committee is the truth, the whole truth and nothing but the truth, so help you God?

Mr. GROOVER. I do.

The CHAIRMAN. Please be seated. Again, we thank you for your willingness to testify. Please proceed with your testimony.

## STATEMENT OF JEFFREY GROOVER, INMATE, FEDERAL CORRECTIONAL INSTITUTION, YAZOO CITY, MS

Mr. GROOVER. Good morning, Mr. Chairman, distinguished senators. Thank you. My name is Jeffrey Groover, and I would like to thank you for the opportunity and privilege to speak to the committee today.

I am 43-years old, I'm from West Palm Beach, FL. I have worked in the computer networking and telecommunications fields for the past 18 years. In 1996, I started a small Internet service provider

company that we sold in 1999; then I started a telecommunications and Internet company.

During the following year, I found myself in financial difficulties. The Internet bust had left me in a financial crisis. I began to fraudulently obtain credit to keep my business going and to support my former wife and two small children. I was subsequently caught and convicted in Federal court of unauthorized use of an access device. I was given a substantial Federal prison sentence.

I stole the identities of a few individuals, including Mr. Nelson Doubleday, a wealthy Florida resident and co-owner of the New York Mets. The techniques are lengthy and technical. However, all that I needed was your name and the approximate area where you lived, and in a few hours I could obtain your full name, your address, your date of birth, your Social Security number, your wife's name, your previous address, and any vehicles or property that you owned.

After applying online for a credit card in your name and being approved within a few minutes, I would receive it in a few weeks. Then I would run a complete credit report from any one of the online credit reporting agencies and find out who you had credit accounts with. From there, I could tap into your bank account, providing that I had the right circumstances. I did all this through the Internet.

Everyone is susceptible to this type of fraud. That is not to scare everyone; that is just to make everyone aware that the Internet is to be used with caution, especially senior Internet users. With just a few small changes, it can also be a safer place to do business as well as conduct credit and financial transactions.

I came here to assist my country and in some small way to find redemption for what I've done. I lost my home, my business, my freedom, and most of all, my wife and children, for what I did. The punishment is severe, and rest assure that I will not do it again. However, that will not stop other people from continuing to do this type of crime due to the ease in which it can be done.

I believe, though, that I can provide you with some recommendations that will stop a large portion of these crimes.

One recommendation is this: To require credit reporting agencies to implement a pass-key system in order to access an individual's credit report. This will save billions of dollars each year in credit fraud done through the Internet or otherwise. When an individual applies for credit, they must enter their pass-key authorizing their credit file to be accessed. If the pass-key is incorrect, then their file is locked and further contact with the correct individual will be necessary to unlock it. This will stop this type of fraud at the inception.

Furthermore, procedures should be implemented to allow a consumer to lock their credit file at their instruction from anyone attempting to gain access to it. For instance, if they go on vacation, away on business or an extended hospital stay, at the time they need their credit report they would simply go online and unlock their file. All this could be implemented easily and without major changes to the credit reporting agencies' system.

Although I do not have enough time here now to provide you in great detail on how to prevent these types of crimes, my knowledge and experience is available to you anytime.

I once again apologize to Mr. Doubleday and the other victims and hope they will forgive me. I am happy to be of assistance to you in this matter and will answer any questions you may have, as well as make further recommendations to the committee.

Thank you once again, Mr. Chairman and members of the committee.

The CHAIRMAN. Well, Jeffrey, thank you for that testimony. Again, I must say I do appreciate your willingness to come before the committee this morning and speak as openly as you have about your own actions, but also to offer up suggestions as to how the Internet might be improved.

Can you state for the record the charges you were convicted of and the time that you are currently serving?

Mr. GROOVER. Yes. It was Title 18, United States Code Subsection 1029, unauthorized use of an access device. I was sentenced to 46 months in Federal prison.

The CHAIRMAN. How was the law enforcement in Florida finally able to catch up with you and your unlawful action on the Internet?

Mr. GROOVER. Basically, Senator, law enforcement was able to catch me because not only was I committing criminal activity, I was raising a family and trying to keep a legitimate business going. Had I only been focused on being a criminal, they would have had a much tougher time catching me, if at all. So basically what I am saying is that the people that are doing this type of crime, if they are solely focused on being criminal, then it is tougher to catch them. In my case, I guess you could say no man's legs are long enough to walk on both sides of the fence.

The CHAIRMAN. Well, that and, I am assuming by what you just said, because you were staying in one location and not moving around or attempting to in any way evade the law, did that assist in their being able to catch you?

Mr. GROOVER. Yes, I would say so.

The CHAIRMAN. Why do you think the Internet is becoming the weapon of choice in perpetuating financial crimes in this country?

Mr. GROOVER. The ease of use and the Internet has become ubiquitous throughout the world. So they can move around, criminals can move around easily, and put up a Web site here or do activity anywhere around the world on the Internet and they can contact another individual or another piece of equipment anywhere in the world.

The CHAIRMAN. In your situation, were the victims, like Mr. Doubleday, compensated for their losses?

Mr. GROOVER. Well, I was ordered to pay restitution in the amount of $271,902, and I've been making payments while in prison. In general, the bank and credit card companies lost the money, not as much the individual. I would like to state for the record I was not targeting Mr. Doubleday because he was a senior citizen. That just happened out of chance.

The CHAIRMAN. How much did calculations of the chances that you would be caught play into your decision to commit Internet

fraud? I should say that in the backdrop, Jeffrey, of your talent, your experience on the Internet coupled with what we believe is a more difficult crime to catch people in. How did that all fit into your particular action?

Mr. GROOVER. Well, it's kind of hard to look back at this point, but I believe that I thought I would not get caught because of my expertise in the computer and Internet field. I didn't think that I would lose my family, my business, my possessions. I didn't think I would be put in a human warehouse a thousand miles from my home. I didn't think about all of those things. So it's kind of hard to say what I was thinking about at that time. Had I thought long and hard, I wouldn't have done it.

The CHAIRMAN. Sure. You have mentioned at least one measure and you spoke of possibly others. How would you advise law enforcement in the pursuit of Internet criminals between States. I say that because you said you stood still. If you were intent on a criminal act and if you were operating, if I can use the term, from a criminal mind, you said it would have been much more difficult to catch you, or to catch someone like you. What recommendations do you offer up to law enforcement?

Mr. GROOVER. That is correct. Actually, in explanation, I initially started out trying to pay back the credit that I was using, and I was paying some of it back. But it doesn't always work out that way. So I did stay in one place.

What I would recommend to law enforcement is to set up an Internet crime clearinghouse to coordinate efforts between agencies; to set up an online Internet crime information center where citizens can find out about companies and people that are doing crime on the Internet. The object is, is to keep the criminals running and moving without giving them an opportunity to stay in one place and create large amounts of these frauds that are going on.

The CHAIRMAN. For a young person to be active on the Internet and have certain skills is one thing; for senior citizens who have never ventured on and are now venturing on in great numbers, as both myself and Senator Collins mentioned, what can senior citizens learn from your case of Internet fraud?

Mr. GROOVER. They should learn the following. Deal with reputable companies. Don't give out personal information over the Internet, such as Social Security numbers and birth dates. When in doubt, check out the company. If you can't reach them by phone, they don't publish a physical address on their Web site, they don't exist. Report fraudulent activity right away, and follow up on it. Don't open suspicious e-mail messages or attachments. If you think someone has stolen your identity, immediately inform in writing the credit bureaus, all of your creditors, including credit card companies, and make sure that you state that no credit is to be issued unless you are contacted first.

Also, take a class on Internet use and join a users group in your area, and learn how to share and exchange ideas and information the way it was meant to be done.

If there is any benefit from what I've recommended, let it be that I have helped people to become empowered to protect themselves better from these types of crimes.

The CHAIRMAN. Well, Jeffrey, thank you very much for those suggestions. Now let me turn to my colleague Senator Collins for questions she might ask.

Senator COLLINS. Thank you, Mr. Chairman.

Do you think that you would have been able to commit the financial crimes that you did engage in were it not for the Internet? Prior to the Internet, would you have been able to get access to the information that you needed to steal other people's identities and then use their credit?

Mr. GROOVER. No, Senator.

Senator COLLINS. So this is a crime that you would not have been able to even conduct were it not for the Internet?

Mr. GROOVER. Correct.

Senator COLLINS. One of the problems of identity theft for the victims is that often it takes them a great deal of time to realize that they are victims of identity theft, and by that time, hundreds of thousands of dollars can be charged to their credit cards. How did your victims discover that you had stolen their identities?

Mr. GROOVER. That I'm not exactly clear on, but I would imagine that they probably got a call from a credit card company of some sort and—asking them about a particular charge or something of that nature.

Senator COLLINS. Do you have any other specific recommendations for us on how individuals can protect themselves or what procedures banks or other sources of credit could put in place to help prevent Internet thefts?

Mr. GROOVER. Yes, I do. The first one would be to request a pass code to be used for all online credit card transactions, different from a PIN.

Senator COLLINS. What do you mean by a pass code, exactly?

Mr. GROOVER. Like a word or a phrase or something like that, or even a long number, that would be used that would verify that you are actually the person that is the owner of that credit card. For example, right now if you drop your credit card outside and someone picks it up, they can go right online and start using it. Without—with a code that they would have to use that would be verified in the automatic verification system, they would be required to enter that code, and if they didn't have that code, the transaction would be declined.

Senator COLLINS. Are there any other recommendations you would like to share with us?

Mr. GROOVER. To require all merchants to have their credit cards processed by a U.S. bank and not done offshore. This would prohibit some of the scams that are going on right now in which they are running up let's say $150—or under a ceiling of $150 or $180 in each transaction, and when it's offshore, they don't have to get a clearing for that transaction, and are guaranteed payment. So when it is done offshore, they are going to get their money no matter what, the criminal is, whereas when it's done by—it's processed by a U.S. bank, the credit card companies don't lose anything and neither does the credit card holder.

Senator COLLINS. Thank you very much. Thank you, Mr. Chairman.

The CHAIRMAN. Well, Jeffrey, we thank you very much again for your willingness to testify, your openness and your candidness as to what we might do to assist in stopping either the criminal or, obviously, someone who finds themselves in a situation, as you did, where you acted in a criminal way to assist yourself. So we do appreciate that very much, and we can ask you to stand down. Thank you.

Mr. GROOVER. Thank you.

The CHAIRMAN. We would ask our second panel to come forward, please.

Good morning, everyone. We appreciate our second panel being with us. Let me introduce them to the committee.

David Nahmias, Deputy Assistant Attorney General for the Department of Justice, Criminal Division; Lawrence E. Maxwell, Assistant Chief Inspector for the U.S. Postal Inspection Service; Howard Beales, Director of the Bureau of Consumer Protection for the Federal Trade Commission; Tanya Solov from the Chicago Secretary of State's Office, representing the North American Securities Administrators Association; and Dave Jevans.

Mr. JEVANS. Jevans.

The CHAIRMAN. Jevans, like Evans.

Mr. JEVANS. Just like Evans, but with a J.

The CHAIRMAN. All right. Thank you. Chairman of the Anti—this is a fascinating term, Senator—Phishing Working Group, who is working closely with the finance and e-commerce industry on Internet crime. In this instance, "phishing" is pronounced—or spelled p-h-i-s-h-i-n-g. David, be willing and able to explain yourself on that one. All right? Fine.

Dave, we will start with you. Please proceed.

**STATEMENT OF DAVE NAHMIAS, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE, WASHINGTON, DC**

Mr. NAHMIAS. Good morning, Mr. Chairman. I am pleased to have this opportunity to appear before this committee and discuss what the Department of Justice is doing to combat Internet fraud, with particular regard to its impact on senior citizens. I have submitted written testimony for the record, which I will briefly summarize now.

As Howard Beales of the Federal Trade Commission can discuss in more detail, Internet use by all demographic groups, including seniors, continues to increase rapidly. Unfortunately, Internet crime is increasing even more rapidly, with both Internet fraud complaints and identity theft complaints filed with the FTC tripling in the past 3 years. Scams ranging from bogus investment deals to schemes that exploit online auctionsites are widely prevalent on the Internet and pose serious risks to the financial well being of senior citizens and other Internet users.

The Department of Justice and our law enforcement and regulatory partners take these trends very seriously, and we have devised a number of responses that includes an aggressive program of criminal enforcement. Last year, for example, the Department spearheaded two nationwide takedowns of prosecutions directed at online economic crime. Operation E-Con, announced in May 2003,

and operation Cyber Sweep, announced in November of last year, involved the combined total of more than 215 criminal investigations directed at schemes that victimized more than 214,000 people out of more than $276 million. These operations resulted in the arrest or conviction of more than 255 people, including more than 70 indictments stemming just from Operation Cyber Sweep in November.

These two takedowns included prosecutions of large-scale Internet fraud schemes involving bogus investments, phishing and other identity theft schemes, fraudulent online pharmaceutical sales, and other cases in which senior citizens and others were at risk of loss or harm. In Operation E-Con, for example, one case successfully prosecuted by the U.S. Attorney's Office for the Eastern District of California involved an online Ponzi scheme known as the Tri-West Investment Club, which took in nearly $60 million from 15,000 investors worldwide. Another online Ponzi scheme that Operation E-Con shut down defrauded more than $8 million from 23,000 investors.

These online investment frauds are of particular concern for seniors, who seek financial information online more than any other group of Internet users and who typically have more assets to lose and less opportunity to recover from losses.

The Federal courts generally appear to be handing down significant sentences for these offenses. For example, in one case of phishing that the U.S. Attorney's Office for the Eastern District of Virginia prosecuted as part of our Operation Cyber Sweep, the lead defendant received 46 months imprisonment and her confederate was sentenced to 37 months in prison.

In another Cyber Sweep identity theft and fraud case prosecuted by the U.S. Attorney's Office for the Southern District of New York, one defendant, who with his co-conspirators had stolen banking and pedigree information which they then used to open PayPal accounts and fund those accounts by direct transfers from victim bank accounts, received 30 months imprisonment. A codefendant is awaiting sentencing. All those sentences, of course, in the Federal system are without parole.

Currently there are several Federal sentencing guideline enhancements that may enable prosecutors to seek higher sentences in fraud cases where senior citizens are victimized. But these enhancements sometimes do not capture the full harm done, especially by identity theft. The administration, therefore, has supported the Identity Theft Penalty Enhancement Act, S. 153, which would create a new offense of aggravated identity theft to ensure a minimum 2-year sentence enhancement in a variety of serious fraud-related offenses and would expand the scope of the existing identity theft statute, 18 U.S.C. Section 1028(a)(7). The Senate has passed that bill, and this morning one of my colleagues from the Criminal Division is testifying before a subcommittee of the House Judiciary Committee in support of the House version of that act.

The successes that we have had to date against online fraud would not have been possible without support from and close coordination with many law enforcement and regulatory partners. I am pleased to say that the FTC, through its outstanding Consumer Sentinel data base of consumer complaints and its enforcement ef-

forts, has been a valued partner in the takedowns I discussed, along with the Postal Inspection Service, the FBI, the U.S. Secret Service, the Bureau of Immigration and Customs Enforcement, and other Federal, State, and local agencies.

We also work closely with foreign governments, such as Canada and Nigeria, and with private sector groups such as the Anti-Phishing Working Group.

Finally, training our prosecutors and investigative agents about Internet fraud and educating the public about how to prevent and avoid Internet fraud are key pieces of our overall enforcement strategy.

Mr. Chairman, that concludes my opening remarks. I would be happy to take questions from the committee now or after all the witnesses on this panel have testified, as you prefer.

[The prepared statement of Mr. Nahmias follows:]

# Department of Justice

STATEMENT

OF

DAVID E. NAHMIAS
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

CONCERNING

INTERNET FRAUD AFFECTING SENIORS

PRESENTED ON

MARCH 23, 2004

Good morning, Mr. Chairman. I am pleased to have this opportunity to appear before the Committee and talk about the role that the Department of Justice is playing to combat Internet fraud, with particular regard to senior citizens.

**BACKGROUND**

There is no question that the Internet has become increasingly attractive to all segments of the population as a medium for everyday information-gathering, communication, and commercial activity. A 2003 report by the Pew Internet and American Life Project shows how popular the Internet has become. As of August 2003, 63 percent of all adult Americans – 126 million people -- now go online, and 52 percent of those Internet users – 66 million people -- go online on a typical day. Older adults are a significant component of this growth. In August 2003, according to the Pew Internet Project, 59 percent of people age 50 to 64, and 22 percent of people age 65 and older, had become Internet users, and those numbers will continue to increase.

It is also important to note the types of online activities in which Internet users routinely engage. For example, according to the Pew Internet Project, online auction participants have almost doubled since 2000 – from 13 million bidders and purchasers in March 2000 to nearly 24 million by December 2002. In addition, the number of people who have tried some form of online banking increased by 127 percent from March 2000 to October 2002, the number of people who have made purchases online has increased by 63 percent since 2000, and about one in ten Internet users has bought or sold stocks online. Finally, the number of Internet-using seniors who search for health information online or do online banking has increased by 20 percentage points since 2000.

Not surprisingly, law enforcement in recent years has witnessed a corresponding growth in online criminal fraud. The Federal Trade Commission (FTC), which receives complaints on

both identity theft and Internet fraud, has noted that the numbers and percentages of identity theft complaints and Internet fraud complaints filed with the FTC have increased greatly in the past three years. Identity theft complaints have nearly tripled in the past three years, from 86,212 in 2001 – 39 percent of all complaints filed with the FTC – to 214,905 – 42 percent of all complaints -- in 2003. It is important to note that identity theft now includes such online criminal techniques as "phishing" – schemes in which criminals set up emails and websites designed to look like those of legitimate companies and financial institutions, then induce people to disclose bank and financial account data, as well as personal data, that can be used in identity theft and fraud. I understand that David Jevans of the Anti-Phishing Working Group will discuss phishing schemes in greater detail in his testimony today.

Internet-related fraud complaints filed with the FTC have also tripled, from 55,727 complaints (42 percent of all complaints) in 2001 to 166,617 complaints (55 percent) in 2003. Both the FTC and the Internet Crime Complaint Center – a joint venture of the FBI and the National White Collar Crime Center -- report that Internet auction fraud has remained the most frequently reported type of online fraud. The Internet Crime Complaint Center reported in 2002, for example, that auction fraud accounted for 46.1 percent of all fraud complaints that it referred to law enforcement.

Other types of online fraud capable of harming seniors have also remained highly prevalent. For example, the Internet Crime Complaint Center reported in 2002 that non-delivery of merchandise or payment for goods ordered online made up 31.3 percent of all referred fraud complaints. We also understand that the Securities and Exchange Commission's Office of Internet Enforcement receives an average of approximately 1,000 complaints per business day.

While a substantial number of these complaints involve non-Internet-related securities fraud, many complaints stem from large-scale spamming of fraudulent or questionable securities-related e-mails to prospective investors in all demographic segments.

At present, our prosecutions of Internet fraud cases indicate that the people behind the schemes range from individuals with no prior criminal records to organized groups, both domestic and international in scope. Although we are not aware of specific cases in which traditional organized crime groups such as La Cosa Nostra or motorcycle gangs organized or conducted the schemes, federal law enforcement is continuing to watch closely for any indications that such groups are becoming involved in online fraud.

**DEPARTMENT OF JUSTICE PROSECUTION OF INTERNET FRAUD**

The Department of Justice is strongly committed to combating all forms of Internet fraud, and to protecting senior citizens from criminals who may seek to target them for any type of fraud. It should be noted that investigation of any Internet fraud scheme, including those affecting seniors, often must overcome several challenges in order to make prosecution of the offenders possible. Investigators, first of all, must amass evidence that makes it possible to attribute behavior, including criminal behavior, to individuals. This task is often a formidable one because of the technology of the Internet, which can enable criminals to conduct their activities with anonymity. Second, the global reach of the Internet not only enables criminals to conduct schemes across multiple jurisdictions, but complicates the task of finding and accessing relevant evidence from those jurisdictions. For example, nearly one-fourth (23.3 percent) of the Internet fraud perpetrators identified by the FBI in 2002 were located outside the United States. Third, investigators must be able to locate and obtain Internet-related evidence quickly, as critical

evidence in the possession of Internet service providers and other e-commerce companies may be preserved for only short spans of time. Fourth, even after they have obtained access to relevant electronic data, the sheer volume of those data may enhance the difficulty of finding the most probative evidence among those data.

I should also note that, as more seniors become computer literate and go online, those seniors who are relative novices are, of course, more susceptible to computer crimes, other than fraud, based on computer intrusions. Their computers may be compromised by hackers who want to steal their data, hijack their computers in order to churn out spam, launch denial of service attacks against others, or carry out other crimes. In addition, seniors who are novice computer users may be more vulnerable to viruses and worms and may, unwittingly, contribute to the spread of such malicious code. These issues involving seniors and the Internet are also concerning.

As part of our coordinated efforts to combat Internet fraud, since 2001 the Department, in coordination with the FBI, the Postal Inspection Service, the Federal Trade Commission, and other law enforcement agencies, has conducted three nationwide "takedowns" of Internet fraud cases. The first of these takedowns, "Operation Cyber Loss" in 2001, involved investigations of online fraud schemes in which more than 56,000 victims lost more than $117 million, and resulted in criminal charges against approximately 90 individuals and companies. In May 2003, we announced the take-down of Operation E-Con, which involved more than 90 investigations of fraud schemes in which 89,000 victims lost an estimated $176 million, and led to the arrests or conviction of more than 130 individuals. Most recently, in November 2003, Operation Cyber

Sweep involved the arrests or convictions of more than 125 individuals and the return of more than 70 indictments directed at some of the leading types of online economic crime.

These takedowns included prosecutions of large-scale Internet fraud schemes involving bogus investments, "phishing" schemes and other identity theft, online auction frauds, and other cases in which senior citizens and others were at risk of loss or harm. Here are a few examples of these prosecutions:

**Online Investment Fraud**

One type of online fraud that poses a particular threat to seniors is investment fraud. Seniors seek financial information on-line more than any other group of Internet users. And seniors who entrust substantial funds to a fraudulent investment opportunity not only lose savings that may be essential for their current needs, but often have fewer opportunities and less time to recoup those funds. Indeed, the proportion of individuals who report losses of more than $5000 from Internet fraud is highest for those age 60 and older.

As part of Operation E-Con in 2001, the United States Attorney's Office for the Eastern District of California indicted two defendants on fraud- and money laundering-related charges relating to one of the largest Internet investment fraud cases in the country. The Tri-West Investment Club was an Internet-based investment fraud scheme that netted approximately $60 million from 15,000 investors worldwide. Tri-West solicited investments in what the website termed a "Bank Debenture Trading Program" or "Prime Bank" note program. The website guaranteed investors a 120 percent annual rate of return with "no risk of losing the investor's principal investment," as well as substantial referral fees for directing others to the website. The case alleged that these investment instruments were nonexistent. According to the indictment,

Tri-West never actually invested any of the investors' money in any "prime bank note" program, but instead used new investor funds to make "dividend" payments to earlier investors to give the false impression of profitability – a classic Ponzi scheme. The balance of the funds were used by the two defendants and others to purchase millions of dollars of real properties in Mexico and Costa Rica, as well as a yacht and helicopter, and to funnel money to dozens of shell companies created in Costa Rica to conceal the defendants' ill-gotten gains.

The indictment also sought the forfeiture of millions of dollars of real properties in Costa Rica and Mexico, a yacht, a helicopter, over a dozen cars, and millions of dollars in bank accounts in Latvia, Mexico and Costa Rica. The two defendants, who were extradited from Costa Rica to Sacramento in December 2002 to face federal charges, have since pleaded guilty, are cooperating with authorities, and remain in custody pending sentencing. A third defendant, Cary Waage, pleaded guilty in 2002 to separate charges relating to Tri-West, is cooperating with authorities and remains in custody pending sentencing. Other individuals allegedly connected with the operations of Tri-West remain fugitives.

Another Operation E-Con case involved a prosecution by the United States Attorney's Office for the District of Colorado. In this case, the defendant was indicted on 15 fraud-related counts pertaining to his alleged operation of an Internet-based Ponzi scheme that took in more than $8 million from 23,000 investors. The defendant allegedly used a website to offer investors an opportunity to become "members" of an offshore investment program run by a company called J&K Global Marketing Corporation. He allegedly promised that if an investor paid a yearly "membership fee" of $375 and waited six months, he or she would receive payments of $375 per month. He also allegedly told investors that he was investing in "high-yield programs,"

which would return between 200 percent and 1200 percent per month. As a result, investors allegedly transmitted membership fees to bank accounts in the United States, Canada, Luxembourg, and the West Indies. The defendant has since agreed to plead guilty and is expected to enter his plea next month.

**"Phishing" Schemes and Other Identity Theft**

Another type of fraud-related crime that may have special impact on seniors is identity theft. Because they often have accumulated substantial financial assets during their years of employment, seniors may have bank and other financial accounts that criminals can easily drain once they have obtained personal and financial data from those seniors through identity theft. Moreover, because many seniors have paid off their mortgages and buy new cars less frequently, they may be less likely to order or review their credit reports in connection with a home refinancing or large-scale consumer purchase. This means that they may be less likely than some younger homeowners and consumers to detect that they have become identity theft victims.

In Operation E-Con, the United States Attorney's Office for the District of Maryland obtained an indictment against two defendants for devising and executing a scheme to lure unsuspecting bank customers to "spoofed" bank websites. At these websites, customers would enter confidential account data that would be transmitted to the defendants, who would use the data to produce and fraudulently use ATM and credit cards. One of these defendants, whose case was transferred to the District of Connecticut, pleaded guilty to bank fraud and wire fraud charges and is awaiting sentencing. The other defendant, a foreign national, is a fugitive – again demonstrating the trans-national nature of these cases.

In another E-Con case, the United States Attorney's Office for the Western District of Pennsylvania obtained an indictment against a defendant on charges of conspiracy, bank fraud, and access device fraud. According to the indictment, the defendant fraudulently used the names, Social Security numbers, and other identifying information from two individuals to apply over the Internet to obtain bank loans and credit cards in the other people's names, and made fraudulent online purchases. On May 23, 2003, the defendant was sentenced to 21 months imprisonment and approximately $25,000 in restitution.

In Operation Cyber Sweep last year, the United States Attorney's Office for the Eastern District of Virginia obtained a guilty plea from a woman on charges of conspiracy to possess unauthorized access devices. The defendant had engaged in "phishing" by sending fake e-mail messages to America Online (AOL) customers, advising that they must update their credit card/personal information on file with AOL to maintain their accounts. Unwitting victims provided their information to the defendant and her co-conspirators. Subsequently, the defendant was sentenced to 46 months imprisonment. One of her co-conspirators previously had pleaded guilty to the same charge and was sentenced to 37 months imprisonment.

In a second Cyber Sweep case, the United States Attorney's Office for the Southern District of New York obtained guilty pleas from two individuals to charges of conspiracy and identity theft for their roles in an Internet fraud scheme that exploited the online payment service PayPal and financial institutions. The defendants and their co-conspirators stole banking and pedigree information from one of their employer's payroll office. They then used the information to open PayPal accounts, and fund the PayPal accounts by direct transfers from the victims' bank accounts to PayPal. Thereafter, they used the fraudulently-funded PayPal accounts to purchase

various items on eBay, and then they sold many of those items on eBay for cash. One defendant pleaded guilty to conspiracy and access device fraud charges on January 23, 2004, and was sentenced to 30 months imprisonment. The other defendant also pleaded guilty to conspiracy and access device fraud charges on October 10, 2003, and is scheduled to be sentenced next month.

In a third Cyber Sweep case, the United States Attorney's Office for the Eastern District of Michigan obtained a criminal complaint and arrest of an individual for credit card fraud, where the Internet was allegedly used to order more than $9,000 in airline tickets. The defendant was a former hotel desk clerk who had access to hotel guests' credit-card numbers and other personal data. The tickets were allegedly purchased using stolen credit-card information from 12 victims using Expedia.com and Lodging.com. The investigation of this case is continuing.

Online Auction Frauds

One of the most common types of Internet fraud involves online auctions. While only a small proportion of seniors (15 percent) who use the Internet report engaging in such auctions, those who do remain vulnerable to this type of crime.

In Operation E-Con, the United States Attorney's Office for the Western District of Pennsylvania obtained a plea of guilty from a defendant to a charge of conspiracy to commit mail fraud and wire fraud. The defendant, who was originally from Belarus, participated in a mail and wire fraud scheme that had two interconnecting parts. The first part of the scheme was that members of the conspiracy hacked into eBay's computer system and logged onto the system as if they were someone who had previously sold items and received favorable ratings from

purchasers of those items. Once a seller received a favorable rating, it was much easier to sell items because there was a proven track record of delivering what was promised.

Members of the scheme then put items up for auction pretending that they were sellers with the proven track records. The successful bidder in the auction was directed to send certified checks or money orders to an address in Pennsylvania, but no items were delivered. The second part of the scheme involved the unauthorized use of credit card numbers to purchase items online that were then shipped to addresses in Pennsylvania. These items were then repackaged and sent to addresses in California. The addresses in Pennsylvania were set up by two co-conspirators, also originally from Belarus, who used false identifications. These two individuals, who worked under the defendant's direction, would stay in apartments for approximately two weeks at a time and receive products and checks at those locations. They would then move to a different apartment and, again, receive checks and products. They moved to a total of four different apartments during the course of the conspiracy until they were arrested by the Pennsylvania State Police. On July 10, 2003, the defendant was sentenced to 18 months imprisonment.

In Operation Cyber Sweep, the United States Attorney's Office for the Eastern District of Missouri obtained an indictment against three individuals for conspiracy to commit wire fraud. According to the indictment, between October 2, 2002 and February 13, 2003, the three defendants monitored Internet-based auctions for sporting event and concert tickets on systems such as eBay and identified losing bidders. Thereafter, one or more of the defendants would send a form letter e-mail message to losing bidders informing them of the availability of additional tickets and inviting those bidders to purchase such tickets from one of them. When a bidder responded to an e-mail invitation to purchase tickets, the bidder was instructed how to pay for the

tickets, typically by way of a Western Union money transfer. In other cases, one or more of the defendants fraudulently solicited bids for event tickets using auctions on eBay. Winning bidders were typically notified by e-mail that the winning bidder was required to make a substantial payment of funds, typically by way of a Western Union transfer of money, before any tickets would be delivered. The indictment further alleged that, upon receipt of money from a bidder, the defendants would keep the proceeds but did not deliver tickets to the bidder. The events included tickets for a Bruce Springsteen concert, tickets for the Fiesta Bowl, tickets for the 2002 SEC Championship football game, and tickets for a Los Angeles Lakers basketball game. All three defendants have since pleaded guilty to the indictment and are scheduled for sentencing next month.

**Online Pharmaceutical Sales**

The Department of Justice has brought a number of criminal prosecutions against individuals who engage in fraudulent sales of drugs and medical devices that may put senior citizens at risk. A very high proportion – 74 percent – of seniors who use the Internet seek health information on-line. Because seniors are highly sensitive to the cost of prescription drugs, seniors may be especially vulnerable to websites or emails that falsely claim to offer safe and effective drugs at what seniors consider affordable prices. Moreover, in some cases senior citizens may be disproportionately harmed if they seek to purchase needed drugs or medical supplies from fraudulent websites.

In Operation Cyber Sweep, the United States Attorney's Office for the Middle District of Louisiana obtained an indictment against a college student on charges of wire fraud relating to his alleged online sales of prescription drugs. The indictment alleges that the defendant, utilizing

the email address Hydrocodone@anywhereUSA.com, posted several messages on a bulletin board owned by www.healthboards.com advertising the sale of prescription pain pills. In February 2003, an FBI agent, acting in an undercover capacity, began sending e-mails to the defendant and arranged to purchase Morphine, Oxycodone, Hydrocodone, Skelaxin and Percocet. The agent wired the funds to purchase the drugs to the defendant from a local convenience store in Baton Rouge and requested that the drugs be sent to him in Baton Rouge. The defendant and another individual went to the Western Union Office in Moscow, Idaho and picked up the funds, but the defendant never sent the drugs ordered by the undercover agent. The case was subsequently transferred to the District of Idaho, where the defendant has pleaded guilty and is scheduled to be sentenced this week.

Just last week, the United States District Court for the Eastern District of Virginia sentenced a pharmacist to 60 months imprisonment and a $140,318 fine for conspiring to violate the Controlled Substances Act and the Federal Food, Drug, and Cosmetic Act in connection with the illegal sale of controlled substances and other prescription drugs over the Internet to consumers through various websites.

* * * * *

There are at least five factors have made it possible for the Department to bring so many successful prosecutions against various forms of Internet fraud. First, several provisions in the Federal Sentencing Guidelines make it possible, in fraud cases involving seniors, to seek higher sentences. Under Section 3A1.1 of the Guidelines, for example, a defendant may receive a two-level increase if he knew or should have known that a victim was unusually vulnerable or otherwise susceptible to the criminal conduct. This enhancement may apply in online investment

schemes, where seniors and others may be susceptible to promises of financial security. [*See* United States v. Harris, 38 F.3d 95 (2d Cir. 1994), cert. denied, 513 U.S. 1198 (1995).] Under Sections 2B1.1 and 3A1.1, respectively, the Department may seek additional enhancements where a substantial part of the scheme was committed from outside the United States or where large numbers of vulnerable victims were involved.

Second, the Department has an ongoing Internet Fraud Initiative that, among other things, ensures that federal prosecutors and agents receive appropriate training about Internet fraud. The Department's National Advocacy Center conducts basic courses in cybercrime that include training about Internet fraud, as well as more advanced courses that focus exclusively on Internet fraud. The Department also supports investigative agencies' in-service training about Internet fraud by providing speakers from the Department's Criminal Division and various United States Attorneys' Offices.

Third, as part of the Internet Fraud Initiative, the Department plays an important role in fostering national-level and cross-border cooperation among law enforcement agencies, by convening and chairing interagency working groups. At the national level, the Telemarketing and Internet Fraud Working Group includes the Postal Inspection Service, the FTC, and the North American Securities Administrators Association, as well as the FBI, the U.S. Secret Service, and other federal and state law enforcement organizations. In the Waage investment fraud case I discussed earlier, the contacts that this Working Group has developed made possible rapid and effective coordination between state securities administrators, the Securities and Exchange Commission, the FBI, and the United States Attorney's Office for the Eastern District of California in the criminal investigation and prosecution. At the international level, the

Department co-chairs the United States - Canada Working Group on Cross-Border Mass-Marketing Fraud, which facilitates similar coordination between U.S. and Canadian law enforcement agencies.

Fourth, the Department recognizes that the successes of initiatives such as E-Con and Cyber Sweep depend heavily on the Department's maintaining close and effective coordination with other federal agencies, such as the FTC and the Postal Inspection Service, on Internet fraud matters. We value our partnerships with the FTC and the Postal Inspection Service in combating Internet fraud and other forms of mass-marketing fraud, such as cross-border telemarketing fraud schemes that target seniors.

Finally, in these Internet fraud takedowns, federal law enforcement has benefitted substantially from cooperation and coordination with foreign governments and the private sector. In the Waage investment fraud case, Costa Rican government authorities made significant contributions in gathering evidence and conducting searches and seizures of property, as well as extraditing defendants. In Operation Cyber Sweep, law enforcement authorities in Ghana and Nigeria and the Merchants Risk Council provided significant assistance to the FBI and other investigative agencies in a number of cases. In 2004, the Department has expanded its outreach to and coordination with the private sector on issues such as "phishing" schemes, and, together with the FBI, the U.S. Secret Service, and the Federal Deposit Insurance Corporation, have been participating in meetings with the Anti-Phishing Working Group.

As important as our enforcement efforts are in combating Internet fraud, the Department also recognizes that continuing public education and prevention measures are needed to warn the public, including senior citizens, about various types of Internet fraud. The Department's own

website, www.usdoj.gov, includes a recently posted Special Report about "phishing" schemes (at http://www.usdoj.gov/criminal/fraud/Phishing.pdf), as well as other Special Reports on identity theft and Africa-related email solicitations and an extensive set of webpages on Internet fraud. The Department also strongly supports the FTC's and the Postal Inspection Service's public education and prevention measures affecting Internet fraud, such as the extensive webpages and printed materials they provide to the public on identity theft and consumer frauds.

* * *

Mr. Chairman, that concludes my prepared remarks. I would be happy to take questions from the Committee at this time.

The CHAIRMAN. Thank you, Dave. We will ask questions, either individually or collective, of all of you after the testimony is given. Now let me turn to Lawrence Maxwell, Assistant Chief Inspector, U.S. Postal Inspection Service.

**STATEMENT OF LAWRENCE E. MAXWELL, ASSISTANT CHIEF INSPECTOR, U.S. POSTAL INSPECTION SERVICE, WASHINGTON, DC**

Mr. MAXWELL. Thank you, Mr. Chairman. I appreciate appearing before you, particularly on this very timely and important matter.

I have submitted some lengthy comments comprehensive with——

The CHAIRMAN. All of those become a part of the record. Thank you.

Mr. MAXWELL. Great. I will summarize those here briefly.

This has become more of a concern. In my formative years as an agent, certainly we saw a lot of victimization of elderly in telemarketing and boiler rooms. Back in the years I worked in New York, we investigated many, saw a lot of potential happy lives ruined. As this evolved, today, now with the Internet, as you have just heard, things have become a lot more of concern, with the speed of the Internet and the ease of it. Where I previously worried about the generation before me, now, as I approach those years, I am starting to worry about myself as well and my generation. We face the same issues.

The Inspection Service enters in—I will just briefly give you a history. We mirror the long, colorful history of the United States. We were formed by Benjamin Franklin. We were formed to protect the Postal Service and, as it turned out, we were the only Federal agents at the time that could serve in the hinterland protecting mail shipments, anything of secure value. Of course, we have had a colorful history battling stage coach robberies and train robberies.

As we came into the modern era, the inspectors became very much involved, in their continued fight to protect the Postal System's carriers from robbery attack, but we also have a reputation for protecting the consumer. That is equally important, as initially all correspondence, all communications, all business was conducted via the mail.

So Congress in the 1870's enacted the Mail Fraud statute, which today remains favored by prosecutors. It is a tremendous statute, has great potential even in this modern era. In fact, it was not until a hundred years after its enactment that it was even modified. That was not to give it more teeth, it was actually to give it more reach. In 1994, I believe, with the crime act, it was modified to extend to private couriers. So it still remains a very viable weapon in our arsenal.

As I said, our focus continues to be to protect the American consumer. We pride ourselves in that. We reach every home in America, every business in America with delivery. We have a profound responsibility to the American public.

Our fraud program consists primarily of about 300 inspectors. We are 1,900 strong; we are one of the smaller Federal agencies. We are funded purely through the Postal Service, so we have a lit-

tle room for growth, but we have to learn to do things smartly and we have to find creative ways to help us in that quest.

Our arrest statistics throughout my career have pretty much stayed on par with what they were in prior years. We investigate roughly 3,000 or 4,000 fraud cases a year of all different types, primarily investment schemes, advance fee schemes. Of course now we are venturing into identity theft. As you just heard it is the fastest-growing crime in America. We make about 10,000 arrests a year.

What we do not pride ourselves on is the concept more-is-better in terms of arrest. What we have learned, and this is almost heresy coming from a law enforcement officer, but what we have learned is the less arrests we can make, as long as we prevent the crime, fewer people are hurt. That is where our focus has been. I know Senator Collins is aware of this from prior campaigns we have conducted. I will just give you an example.

Some of the cases we have had in mail fraud—and we have had cases resulting in, just last year, $2 billion in court-ordered restitution to consumers that were victimized in fraud—we forfeited $36 million. We put our forfeiture funds back into our fight against crime, much of which goes to our prevention efforts. But through some creativity several years ago, creativity and vision by a U.S. attorney and by the Postal Inspector agents, they approached us about formulating a special account with funds earmarked for fighting fraud, the thought being fraud is the one crime you can actually educate someone to protect themselves. We bought into that concept in a considerable way, and I still believe very strongly in fraud prevention through consumer education.

As you consider the Internet and the senior citizens now venturing on the Internet—and I read some studies where Direct Mail quoted 75 percent of homes in America now have Internet access, which sounds high to me but certainly not shocking. As more people venture onto the Internet, the seniors that go on, certainly if they are smart enough to navigate the Internet, they are smart enough to be educated and taught how to protect themselves.

As I said before, what is old is new today. So what is new on the Internet really is not new. We just have to teach people to find ways to see fraud as they encounter electronically. The Internet is a lot faster than the written word or mail solicitation.

What we have done is, of course, to partner. You have heard in prior testimony, Operation Cyber Sweep. We were proud to be part of that. Project kNOw Fraud in 1999, with our friends from FTC, probably our strongest partners in this fight. They are very consumer-oriented, we share our databases, we try to go to that concept of one-stop shopping for the victim, because in No Fraud we learned that most consumers do not know where to complain. It is kind of tragic that, you know, you have all of these complaints, or possibly good criminal intelligence, and we are not made aware of it.

Just last year, in the National Fraud Against Senior Fraud Awareness Week, which was a result of our approaching Senator Collins and Senator Levin who passed a resolution declaring Senior Fraud Awareness Week then conducted a campaign using literature which I have put outside, the hearing room which is very

effective. I applaud your efforts for that support and hope to see more of these cooperative initiatives in the future. Any time you have an event of that media attention and public information, it is a great way to get the word out. It is a way of reaching people.

What we have done with several of the cases that I mentioned earlier, monies coming from forfeitures and fines were directed by the court and by the U.S. attorney, in agreement with us, to put into this special consumer protection fund. Those are the monies that we have used for Project kNOw Fraud, which I mentioned earlier, for our campaign around the senior fraud awareness week. We are also applying it—again, with identity theft, we have a tremendous potential with the Internet, both with "phishing" and "spoofing", as I think will be covered in greater depth later. We have had several cases which involve identity theft. It is not only, as you mentioned in the first testimony, when people become aware, it is how long it takes to correct the problem. For example, one in their golden years certainly do not need that torment as they go on through the last decades of their life.

We did produce a professionally done DVD video, which is about 12 minutes in length. We have a number of them outside. If you have not seen it, I would encourage you to view it. It is very well done, if I say so myself, but we had some professionals help. It presents in a very short way but a dramatic way what you should look for to protect against identity theft. It leaves you with an impact.

What I would leave the panel and certainly open up to questioning is my view on this education and prevention remains strong. If there is a way to funnel funding for agencies to continue this, either through fines, perhaps through forfeiture, I would welcome that and certainly be happy to work toward that effort. There are other powers we probably could use that might help on the Internet. It is a little more of a difficult problem than what we faced with the West African 419 letter, for instance. Those were actual tangible letters. We seized about 5 million of them after we reached agreement with the countries of Nigeria and Ghana, and we were able to destroy them before they did the damage.

However, what happened, was when they realized we were stopping them from getting their pitch to their victims, they moved onto the Internet. That is a little tougher challenge for us. So we have some thoughts on that, but anything you or the committee could recommend would be greatly welcomed by us.

I thank you for your time.

[The prepared statement of Mr. Maxwell follows:]

**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.

The CHAIRMAN. Lawrence, thank you very much for your testimony. Now let us turn to Howard Beales, Director of the Bureau of Consumer Protection for the Federal Trade Commission.

Howard, welcome to the committee.

**STATEMENT OF J. HOWARD BEALES, III, DIRECTOR, BUREAU OF CONSUMER PROTECTION, THE FEDERAL TRADE COMMISSION, WASHINGTON, DC**

Mr. BEALES. Thank you, Mr. Chairman, and thank you, Senator Collins. I look forward to this opportunity to provide our testimony about Internet fraud and its effect on senior citizens.

The Internet is one of the most revolutionary marketing and communications tools that we have seen in a long time and it plays an increasingly central role in consumers' lives. Unfortunately, as consumers have turned to the Internet, so too have scam artists. Last year, for the first time, Internet-related fraud complaints exceeded other fraud complaints, comprising 55 percent of all fraud complaints. It was also the first year in which consumers reported that the Internet outstripped the telephone as the point of their first contact with the fraudulent scheme.

However, Internet fraud does not yet appear to be affecting seniors age 60 and over as much as other age groups. During 2003, only 28 percent of the complaints from seniors concerned Internet-related fraud, and only 6 percent of the Internet-related fraud complaints from all consumers came from seniors. Moreover, seniors continue to report that their first contact with scammers came predominantly by telephone. In our experience, Internet scams generally do not target the elderly as a specific group, but they seek consumer victims regardless of demographic criteria.

Nonetheless, Internet scams that cause significant financial injury can be particularly devastating to seniors, many of whom live on limited or fixed incomes. Scams that facilitate identity theft are of particular concern. ID theft strikes all segments of the population, and it is not surprising to find that older Americans are also targets of this crime.

Although consumers who are age 60 or over are no more likely to become victims of identity theft, the crime appears to affect them in distinct ways. For example, while 33 percent of all consumers who filed ID theft reports experienced some sort of credit card fraud, 44 percent of those 60 or older were victims of credit card fraud. A greater percentage of older Americans reported ID theft attempts to the FTC than did the general population.

Under our civil law enforcement authority, the FTC has brought actions to stop practices that involve or facilitate identity theft. Our cases have attacked pretexting, where scammers use false pretenses to obtain consumers' confidential financial information. We have also attacked phishing, where criminals use spam to trick consumers into revealing confidential payment information. These schemes use Web sites that appear identical to the sites of legitimate companies with whom consumers do business, and they as consumers to update or validate their information. In fact, just yesterday the FTC and the Department of Justice announced a joint law enforcement initiative that shut down a phishing scheme.

Last year, auction fraud accounted for nearly half of all Internet-related fraud complaints consumers reported to the FTC. Among consumers age 60 and over, it was 29 percent of all Internet-related complaints and ranked third in the top 15 product or service complaints reported by consumers. In light of this data, the Commission launched Operation Bidder Beware, an enforcement sweep targeting Internet auction scams. The sweep combined the efforts of the FTC, 29 participating State attorneys general, and numerous local law enforcers. Working together, we brought more than 50 criminal and civil enforcement actions against various Internet auction scams. We also kicked off an extensive Federal-State consumer education campaign featuring a dedicated Web page with information on how to avoid auction fraud.

Another source of misleading Internet promotions is products or services that promise to cure or treat serious diseases or conditions such as cancer, heart disease, arthritis, and diabetes. Older consumers constitute a large part of the market for health-related services and remain vulnerable to misleading claims and fraudulent practices.

To address these problems, we launched Operation Cure-All, a coordinated FTC, law enforcement, and consumer and business education initiative with a bilingual Web site. Last month, the FTC announced a final order banning a Canadian company from offering a sham cancer therapy on its Internet Web site which referred U.S. citizens to the company's clinic in Tijuana, Mexico, a true North American free fraud.

One of the problems in prosecuting Internet fraud is that the Internet knows no boundaries, and cross-border fraud on the Internet is a serious problem. In 2003, 47 percent of cross-border complaints involved the Internet, up from 33 percent the year before. To date, the Commission has had foreign targets in over 60 cases and pursued assets offshore in more than 10 foreign countries. To enhance our ability to pursue these cases, the Commission has recommended a package of legislative changes that will facilitate cooperation with foreign law enforcement authorities. Unless we can build stronger enforcement cooperation across borders, more and more Americans will fall victim to imported fraud.

Internet fraud causes significant injury to consumers and harms public confidence in the Internet as an emerging marketplace. The FTC will continue to combat Internet fraud through aggressive law enforcement and consumer education. To date, the Commission has brought 319 Internet enforcement cases. Because prevention is often the best medicine, the FTC takes an active role in educating consumers about Internet scams. We have developed publications, launched dedicated Web pages, and worked with numerous Federal agencies and private sector partners to develop and disseminate plain-language consumer education materials in English and Spanish to protect all consumers, including seniors, from Internet fraud.

We will continue that effort and we look forward to working with you and the committee on the combating senior fraud initiative.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Beales follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

# EFFORTS TO FIGHT FRAUD ON THE INTERNET

Before the

SENATE SPECIAL COMMITTEE ON AGING

Washington, D.C.

March 23, 2004

## I. Introduction

Mr. Chairman and members of the Committee: I am Howard Beales, Director of the Bureau of Consumer Protection of the Federal Trade Commission.[1] I am delighted to appear before you today to discuss the Commission's efforts to fight unfair and deceptive practices on the Internet that harm all consumers, including the elderly.[2] Internet fraud causes significant injury to consumers, and harms public confidence in the Internet as an emerging marketplace. That is why the Commission has maintained an active law enforcement program, bringing 319 Internet law enforcement cases to date.[3]

The testimony today will discuss the Commission's law enforcement and consumer education efforts to combat fraud and deception on the Internet, addressing identity theft, auction fraud, investment fraud and "Nigerian scams," cross-border Internet fraud. The testimony also discusses the Commission's cooperative efforts with other law enforcement agencies, and provides information about fraud complaints received from older consumers. The Commission is keenly aware that the Internet's development as a virtual marketplace and means of communication for all consumers requires our continuing vigilance and effort.

## II. Identity Theft

Although identity theft may have originated in the offline world, the Internet is also becoming a vehicle for identity thieves. The Commission's primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the ID Theft Act"

---

[1] The views expressed in this statement represent the views of the Commission. My oral presentation and responses to any questions you have are my own, however, and do not necessarily reflect the Commission's views or the views of any individual Commissioner.

[2] The Commission enforces Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which broadly prohibits unfair and deceptive acts and practices in or affecting commerce, whether in the brick and mortar world or the virtual world of the Internet.

[3] This total includes cases announced as of February 29, 2004.

or "the Act").[4] This statute directed the Commission to establish a central federal repository for identity theft complaints; to make available and to refer these complaints to law enforcement for their investigations; and to provide victim assistance and consumer education. Thus, the FTC's role under the Act is primarily one of facilitating information sharing between public and private entities. The Commission also works extensively with industry on ways to improve victim assistance,[5] including providing direct advice and assistance in cases of security breaches involving sensitive information of customers or employees.

To fulfill the ID Theft Act's mandate, the Commission established a toll-free hotline and online complaint program for ID theft victims. This system achieves two significant goals. First, it provides ID theft victims with immediate access to information and resources that allow them to begin to recover from what is often a devastating event.[6] Second, the complaint information provided by the victims becomes part of the information in the Commission's ID Theft Clearinghouse. This information is made available to more than 850 criminal and civil enforcement agencies throughout the nation through the Commission's Consumer Sentinel network, a secure online tool for data sharing and law enforcement coordination.

Because ID theft strikes all segments of the population, it is not surprising to find that older Americans are also targets of this crime. In 2003, 214,905 complaints were filed in the

---

[4] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

[5] As part of its consumer education and victim assistance program, the Commission has distributed more than 1.3 million copies of its 26-page booklet, *Identity Theft: When Bad Things Happen To Your Good Name*, which also can be downloaded from the ID theft website. *See* http://www.consumer.gov/idtheft. The Commission has created a standard ID Theft Affidavit in both English and Spanish for victims to use in resolving debts.

[6] *See* http://www.consumer.gov/idtheft for the online complaint form and consumer education material.

Clearinghouse.[7] The ID Theft Clearinghouse provides insight into how ID theft affects seniors. Of the nearly 200,000 complaints received in 2003 where victims reported their age, slightly more than 19,000, or about 10%, came from consumers who are age 60 or over.[8]

Although the Clearinghouse data provides a window into current trends in this increasingly common crime, the Commission has collected additional data to aid in its understanding and response to the problem. In 2003, the Commission conducted a nationwide survey to assess the cost and prevalence of ID theft.[9] The results were dramatic. The survey showed that in the course of one year, about 3.2 million consumers had new accounts opened, or other fraud committed, in their names. Another 6.7 million consumers experienced misuse of an existing account. The monetary losses associated with victims trying to repair the damage done by the theft and misuse of their information were equally striking, costing businesses about $48 billion, and consumers $5 billion.[10]

Identity theft appears to affect older Americans in distinct ways. For example, while 33% of all consumers who filed ID theft reports experienced some sort of credit card fraud, 44% of

---

[7] Federal Trade Commission, National and State Trends in Fraud & Identity Theft (January- December 2003) (hereinafter, "National Trends"), p. 4. This publication is available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf.

[8] National Trends, "Identity Theft Complaints by Victim Age," *supra* n.7, p. 11. This percentage is less than the proportion of seniors in the population at large. Population Division, U.S. Census Bureau, Table NA-EST2002-ASRO-01 - National Population Estimates - Characteristics (Release Date: June 18, 2003) (hereinafter, "Census Estimates").

[9] Federal Trade Commission, Identity Theft Survey Report (Sept. 2003). A private research firm conducted a random sample telephone survey of over 4,000 U.S. adults in March and April 2003 for the Commission. The full report can be found at http://www.consumer.gov/idtheft/stats.html.

[10] This does not include time costs. About 16% of the victims surveyed were age 60 or older, which directly reflects their 16.4% representation in the population at large, according to the most recent census data. Census Estimates, *supra* n. 8.

those 60 or older were victims of credit card fraud.[11] On the other hand, 21% of the population reported phone or utilities fraud, while only 16% of seniors reported this problem. Not surprisingly, far fewer older Americans reported employment-related fraud (4%) than the population at large (11%). And a greater percentage of older Americans reported ID theft attempts (14%) to the Commission than did the general population (8%).

Most identity theft cases are best addressed through criminal prosecution, and the Commission refers potential cases to criminal authorities because the FTC Act provides no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, however, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. Our cases have attacked alleged "pretexting," the use of false pretenses to obtain consumers' confidential financial information,[12] and "phishing," the use of spam directing consumers to update or validate their confidential payment information on copycat websites that appear identical to the sites of the legitimate companies with which they do business.[13] Although the Commission works with businesses on information security problems, the Commission has also taken action against companies that

---

[11] *See* National Trends, "Credit Card Fraud," *supra*, n.7, p. 10; Appendix A, p. A-1 It also is worth noting that most of the recent increase primarily involves the account takeover form of identity theft that tends to cause less economic injury to victims and is generally easier for them to identify and fix.

[12] *E.g., FTC v. Corporate Marketing Solutions, Inc.*, No. CIV-02-1256-PHX-RCB (D. Ariz. Feb. 3, 2003) (final order providing $525,000 for consumer redress, banning defendants from telemarketing, and barring false claims of affiliation with banks, credit card issuers, and consumer agencies); *FTC v. G. M. Funding*, No. SACV 02-1026 DOC (C.D. Cal. May 5, 2003) (final order).

[13] *FTC v. C.J.*, No. CIV-03-5275-GHK (RZx) (C.D. Cal. July 24, 2003) (final order barring defendant from sending spam purporting to come from AOL that directed consumers to a "look alike" AOL website where the defendant obtained financial information used for his own online purchases).

misrepresent the level of security they provide and required those businesses to take reasonable and appropriate steps to keep consumers' information secure.[14]

**III. Auction Fraud**

In 2003, auction fraud accounted for the greatest number – nearly half – of all Internet-related fraud complaints consumers reported to the Commission's Consumer Sentinel complaint database.[15] Among seniors age 60 and over, auction fraud accounted for 29 percent of all Internet-related complaints in 2003, and ranked third in the list of "Top 15" product or service complaints reported by seniors. In light of this data, the Commission launched "Operation Bidder Beware," an enforcement sweep targeting Internet auction scams on April 30, 2003.[16] The sweep combined the efforts of the Commission, the National Association of Attorneys General ("NAAG"), 29 participating state Attorneys General, and local law enforcers to bring more than 50 criminal and civil law enforcement actions against Internet auction scams,[17] and

---

[14] *E.g., In re Guess, Inc.*, (FTC July 30, 2003) (consent order available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html); *In re Microsoft Corp.*, (FTC Aug. 8, 2002) (consent order available at http://www.ftc.gov/os/2002/08/microsoftagree.pdf). *In re Eli Lilly*, (FTC Jan. 18, 2002) (consent order available at http://www.ftc.gov/os/2002/01/lillyagree.pdf).

[15] National Trends, "Top Products/Services for Internet-Related Fraud Complaints," *supra* n.7, p. 8 (48%, or nearly 80,000 of the 166,617 Internet-related complaints in 2003 concerned auction fraud). The online Sentinel database is used by 943 federal, state, and local agencies for civil and criminal enforcement cases.

[16] The press release can be found at http://www.ftc.gov/opa/2003/04/bidderbeware.htm. In a prior initiative in February 2000, the Commission, Department of Justice, U.S. Postal Inspection Service, and NAAG members announced the filing of 35 Internet auction fraud cases. *See* http://www.ftc.gov/opa/2000/02/internetauctionfraud.htm.

[17] Commission staff trained hundreds of federal, state, and local law enforcement personnel on techniques to investigate auction fraud. Commission staff also provided investigative assistance for a significant number of cases in the sweep.

kicked off an extensive federal-state consumer education campaign featuring a dedicated web page providing consumers with information on how to avoid auction fraud.[18]

Many of the "Operation Bidder Beware" cases involved straightforward scams where consumers allegedly "won" an Internet auction for computer software and electronics, sent in their money, but never received the merchandise. In one case, for example, two defendants allegedly continued to change their auction account names to conceal the fact that they never delivered promised merchandise, and later embarked on serial identity theft so that defrauded auction bidders would mistakenly blame the identity theft victims. The Commission obtained a permanent injunction banning both defendants from participating in Internet auctions and requiring consumer redress payments of nearly $100,000.[19] The two defendants have since been convicted of mail fraud pursuant to prosecution by the U.S. Attorney's Office for the Northern District of Illinois.[20]

## IV. Investment Fraud and "Nigerian Scams"

The FTC Act gives the Commission authority to pursue many deceptive Internet-related investment scams, which run the gamut from oil and gas leases and FCC license frauds to gemstone, art, precious metals, and rare coin investment schemes. The Commission has successfully pursued several of these scams over the years, as have state and federal criminal authorities. Recently, the Commission has devoted a substantial share of its consumer education

---

[18] The web page can be found at http://www.ftc.gov/onlineshopping.

[19] *FTC v. James D. Thompson, et al.,* No. 03-C-2541 (N.D. Ill. Aug. 21, 2003) (final order).

[20] *U.S. v. Thompson, et al.,* No. 03-CR-745-ALL (N.D. Ill. *filed* July 31, 2003). Defendant Germak is scheduled to be sentenced on March 15; Defendant Thompson, on June 14, 2004.

resources to preventing consumers from being taken in by investment scams.[21] For the last two years, with increased criminal enforcement and the Commission's increased consumer education activities, investment fraud has not appeared among the Consumer Sentinel "Top 15" categories of scams affecting seniors age 60 and over.[22]

Deceptive business opportunities, in contrast, ranked seventh as a source of Internet-related complaints overall in 2003,[23] and business opportunity and work-at-home promotions filled the last two slots of the "Top 15" scams affecting seniors age 60 and over.[24] Consequently, the Commission has actively pursued business opportunity and work-at-home scams by bringing cases and by leading state and federal law enforcement sweeps.[25]

"Nigerian Scams" are a persistent con in which a purported third-world official or businessman typically offers to share his family's fortune with a consumer in return for help in circumventing his country's currency restrictions by moving assets outside his country to a safe banking haven – but only after the consumer sets up a bank account in the scammer's name with a good faith deposit, which soon vanishes. The Commission has issued a Consumer Alert on

---

[21] In 2003, 392 of the 166,617 Internet-related fraud complaints received by Consumer Sentinel concerned investment scams. Appendix A, p. A-4.

[22] Appendix A, p. A-3.

[23] National Trends, "Top Products/Services for Internet-Related Fraud Complaints," *supra* n.7, p. 8.

[24] Appendix A, p. A-3.

[25] In the most recent sweep, "Project Busted Opportunity," state and federal participants brought 77 law enforcement actions. *See* http://www.ftc.gov/opa/2002/06/bizopswe.htm. The Commission also recently announced a stipulated final judgement in an Internet business opportunity case which required the defendants to pay $500,000 in consumer redress for victims. *FTC v. End70 Corp., et al.*, No. 3:03-CV-0950-N (N.D. Tex. Dec. 11, 2003). The press release appears at http://www.ftc.gov/opa/2004/01/bizoppsweep.htm.

Nigerian scams as part of its consumer education mission,[26] and assisted criminal authorities in identifying potential cases.[27] Although the representations made in these solicitations may seem far-fetched to many consumers, consumers who fall prey to this scam suffer significant injury. Taking action against these types of scam artists highlights the cross-border issues that can be addressed by our legislative proposals discussed below.

## V. Cross-Border Internet Fraud

The Internet knows no boundaries, and cross-border fraud on the Internet is a growing problem. During both 2002 and 2003, approximately 14% of the fraud complaints collected in Consumer Sentinel involved a cross-border component.[28] In 2003, 47 percent of these complaints involved the Internet, up from 33 percent in 2002.[29] To date, the Commission has had foreign targets in over 60 cases and pursued assets offshore in more than 10 foreign countries.

Older consumers are often the targets of cross-border fraud. In 2003, consumers 60 and over comprised 20% of all cross-border fraud complaints where consumers reported their age.[30] Top frauds reported by consumers age 60 and over included prize promotions, sweepstakes

---

[26] The alert can be found at http://www.ftc.gov/bcp/conline/pubs/alerts/nigeralrt.htm.

[27] Because Nigerian scams tend to require victims to engage in criminal activity, they are best evaluated and pursued by criminal authorities.

[28] Appendix A, p. A-5.

[29] *Id.*

[30] Appendix A, p.A-6. As of July 1, 2002, persons age 60 and over made up approximately 16.4% of the U.S. population. Census Estimates, Table NA-EST2002-ASRO-01 - National Population Estimates - Characteristics.

scams, foreign money offers, advance-fee loans, and foreign lotteries – all common cross-border schemes.[31]

"Operation Cure.All," an on-going, coordinated Commission law enforcement and consumer/business education initiative with a bilingual website,[32] continues to target deceptive and misleading Internet promotions of products and services that promise to cure or treat serious diseases or conditions affecting seniors and others, such as cancer, heart disease, arthritis, and diabetes. Older consumers constitute a large part of the market for health-related services, and remain vulnerable to misleading claims and fraudulent practices. The Commission strives to ensure that claims (in both traditional media and on the Internet) about the health benefits of over-the-counter drugs, devices, foods, and dietary supplements are truthful, not misleading, and substantiated by competent and reliable scientific evidence. Most recently, the Commission on February 25, 2004, announced a final order banning a Canadian company from offering a bogus cancer therapy on its Internet website which referred U.S. citizens to the company's clinic in Tijuana, Mexico.[33]

The legislative proposals that the Commission has asked Congress to enact would better protect consumers by improving the agency's ability to cooperate and share information in cross-border cases and investigations.[34] The recommendations focus primarily on improving the Commission's ability to combat fraud involving foreign parties, evidence, or assets, and include

---

[31] *See* Appendix A, p. A-3.

[32] The website appears at: at http://www.ftc.gov/bcp/conline/edcams/cureall/coninfo.htm.

[33] *FTC v. CSCT, Inc., et al.*, No. 03-C-00880 (N.D. Ill. Feb. 12, 2004) (final order).

[34] These proposals are reflected in two bills now before Congress – S. 1234 and H.R. 3143.

four main components.[35] First, the Commission seeks to strengthen its ability to cooperate with foreign counterparts, including the ability to share information on a confidential basis and to assist in investigations. Second, the Commission requests enhancements to its information-gathering capabilities, including the ability to obtain information from third parties without triggering advance notice to investigative targets that may prompt them to move their assets offshore. Third, the Commission asks for improvements to its ability to obtain consumer redress in cross-border litigation by clarifying the agency's authority to bring cross-border cases, and expanding its ability to work with the Office of Foreign Litigation of the Department of Justice to pursue offshore assets. Finally, the Commission wants to strengthen international cooperative relationships by obtaining authority to facilitate staff exchanges and provide financial support for joint projects. The Commission's proposals would provide authority comparable to that of various other federal agencies.

## VI. Other Cooperative Internet Enforcement Efforts

The Commission also has cooperated with other government agencies to attack Internet fraud. Working with the Department of Justice and Postal Inspection Service, the Commission has contributed cases to two FBI initiatives targeting Internet scams, "Operation E-Con" in May, and "Operation Cyber Sweep" in November 2003. In one, the Commission obtained $247,000 in consumer redress from defendants who allegedly promised $125,000 in annual earnings from a

---

[35] Although these legislative proposals, if adopted, will significantly assist the Commission in its efforts, difficulties will remain in investigating cross-border fraud cases given differences among foreign countries regarding information-sharing.

prepackaged Internet business that was nothing more than a pyramid scheme requiring purchasers to replicate the defendants' website and sell it to others.[36]

We have also worked closely with criminal authorities on egregious cases of Internet fraud. As recently as February 26, 2004, for example, a federal judge in the Southern District of New York sentenced Commission defendant John Zuccarini[37] to 30 months in prison following his December 10, 2003, guilty plea to a 50 count indictment obtained by the U.S. Attorney.[38] This case, the first of its kind to be brought under the Truth in Domain Names Act of 2003,[39] exemplifies the benefits of interagency cooperation, with significant contributions from the U.S. Attorney for the Southern District of New York, the Postal Inspection Service, and the Commission.

## VII. Internet Fraud and Older Consumers

---

[36] *FTC v. K4 Global Publishing, Inc., et al.*, No. 5:03-CV-0140-3-CAR (M.D. Ga. Oct. 14, 2003).

[37] *FTC v. John Zuccarini, et al.*, No. 01-CV-4854 (E.D. Pa. Apr. 9, 2002) (permanently barring Zuccarini from diverting or obstructing consumers on the Internet and from launching websites or pages that belong to unrelated third parties, advertising affiliate programs on the Internet, and ordering him to pay more than $1.8 million in ill-gotten gains for consumer redress). The Commission had sued Zuccarini for "mousetrapping" consumers who mistyped popular website names. He had registered some 6,000 misspellings of site names as domain names, so that consumers who mistyped a web address would be taken to his sites. Zuccarini's sites took control of their web browsers, forcing them to view dozens of sites that paid him for advertising their adult content, online gambling, and psychic services. To escape, consumers had to spend as much as 20 minutes to close out Zuccarini's pop-up browser windows, or turn off their computers and lose all their "pre-mousetrap" work. *See* Benjamin Weiser, *Spelling It 'Dinsey,' Children on Web Got XXX*, N.Y. TIMES, Sept. 4, 2003, Section B (Late Edition), at 1.

[38] *U.S. v. Zuccarini*, No. 1:2003-CR-01459 (S.D.N.Y. Feb. 26, 2004). The DOJ press release appears at http://www.cybercrime.gov/zuccariniSent.htm.

[39] *See* 18 U.S.C. § 2252B(b).

In 2003, Consumer Sentinel received 301,835 fraud complaints from consumers, 68% of whom volunteered their age.[40] Seniors age 60 and over, who represent 16% of the U.S. population,[41] filed 13% of these complaints.[42] Last year, seniors filed 6,088 Internet-related frau complaints providing payment data, and reported payments of $12.8 million to Internet frauds, with a median loss of $186 per person.[43]

Emerging trends in the Sentinel complaint data highlight the increasingly central role of the Internet in consumers' lives. Internet-related fraud complaints exceeded other fraud complaints for the first time last year, comprising 55% of all fraud complaints.[44] In addition, 2003 was the first year in which consumers reported that the Internet outstripped the telephone as the point of their first contact with a fraudulent scheme.[45]

Internet fraud does not yet appear to be affecting seniors age 60 and over as much as othe age groups. During 2003, only 28% of the complaints from seniors concerned Internet-related fraud,[46] and only 6% of the Internet fraud complaints from all consumers who reported their age

---

[40] National Trends, "Fraud Complaints by Consumer Age," *supra* n.7, p. 7.

[41] Population Division, U.S. Census Bureau, Table NA-EST2002-ASRO-01 - National Population Estimates - Characteristics (June 18, 2003).

[42] National Trends, "Fraud Complaints by Consumer Age," *supra* n.7, p. 7.

[43] Appendix A, p. A-2.

[44] National Trends, "Fraud Complaints by Calendar Year," *supra* n.7, p. 4. In 2002, the reverse was true: Non-Internet fraud complaints comprised 55% of all fraud complaints.

[45] National Trends, "Company's method of Contacting Consumers," *supra* n.7, p. 7. In 2003, 32% of consumers reported that their first contact with scammers came over the Internet; 26%, by email; 18%, by phone; and 13%, by mail.

[46] Appendix A, p. A-2.

came from seniors.[47] Moreover, 44% of seniors continued to report that their first contact with scammers came by telephone, compared to 28% whose first contact was by Internet website or email.[48] This may simply reflect the fact that Internet-savvy baby boomers will not begin turning 60 until 2005.

The Commission recognizes that the American population is aging, and therefore issues facing older consumers are becoming even more pressing. In the Commission's experience, however, Internet scams do not target the elderly as a specific group, but seek consumer victims without regard for demographic criteria. Nonetheless, Internet scams that cause significant financial injury can be particularly devastating to seniors, many of whom live on limited or fixed incomes.

Because prevention is often the best medicine, the Commission takes an active role in educating seniors and others about Internet scams. To that end, the Commission has developed a series of publications, launched dedicated Web pages, and worked with numerous federal agencies and private sector partners to develop and disseminate plain-language consumer education materials in English and Spanish to protect all consumers, including seniors, from Internet fraud.

**VIII. Conclusion**

The Commission is hard at work on efforts to protect all Americans, including the elderly, from Internet scams. Through consumer education outreach efforts and enforcement actions that halt law violations and return money to victims, the Commission seeks both to help consumers protect themselves and to take action when they cannot. The Commission is

---

[47] National Trends, "Internet-Related Fraud Complaints by Consumer Age," *supra* n.7, p. 8.

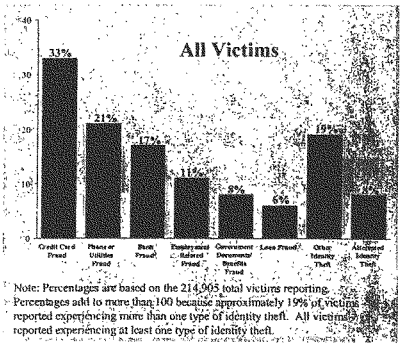
[48] Appendix A, p. A-3.

committed to emphasizing this important work, enlisting the help of private and public partners to maximize the effectiveness of the effort.

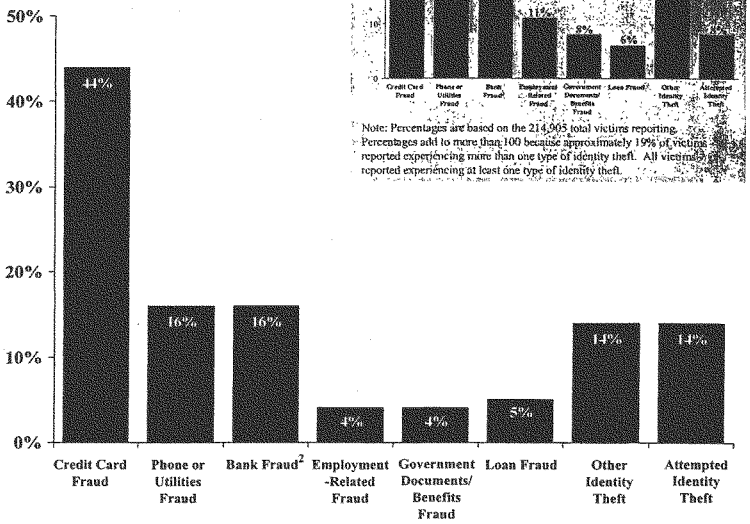
# APPENDIX A

## How Victims' Information Is Misused

*January 1 – December 31, 2003*




**Victims Age 60 and Over[1]**




[1]Percentages are based on the 19,248 identity theft victims age 60 and over who contacted the Federal Trade Commission directly and reported their age. The bars sum to more than 100% because victims can report experiencing more than one type of identity theft.

[2]Includes identity theft fraud involving checking and savings accounts and electronic fund transfers.

## Total Number of Internet-Related Fraud Complaints & Amount Paid for Consumers Age 60 and Over

*January 1, 2001 - December 31, 2003*

| CY | Total No. of Complaints | Complaints Reporting Amount Paid | Percentage of Complaints Reporting Amount Paid | Amount Paid Reported | Average Amount Paid[1] | Median Amount Paid[2] |
|---|---|---|---|---|---|---|
| 2001 | 1,475 | 1,135 | 77% | $1,176,344 | $1,036 | $173 |
| 2002 | 4,105 | 3,494 | 85% | $2,690,618 | $770 | $192 |
| 2003 | 7,384 | 6,088 | 82% | $12,818,313 | $2,106 | $186 |

[1]Average is based on the total number of consumers age 60 and over who reported amount paid (CY 2001=1,135; CY 2002=3,494; CY 2003=6,088). One consumer reported an amount paid of $6.2 million for CY 2003.

[2]Median is the middle number in a set of numbers so that half the numbers have values that are greater than the median and half have values that are less. Calculation of the median excludes complaints with amount paid reported as $0.

## Number of Internet-Related Fraud Complaints from Consumers Age 60 and Over

*January 1, 2001 - December 31, 2003*

| | CY 2001 | Percentage[1] | CY 2002 | Percentage[1] | CY 2003 | Percentage[1] |
|---|---|---|---|---|---|---|
| Total Number of Fraud Complaints from Consumers Age 60 and Over | 6,141 | | 19,789 | | 26,589 | |
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |
| [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] | [illegible] |

[1]Percentages are based on the total number of fraud complaints from consumers age 60 and over by calendar year.

## Company's Method of Contacting Consumers[1]
## Age 60 and Over
*January 1, 2001 – December 31, 2003*

| Initial Contact | CY 2001 No. Complaints | CY 2001 Percentage[1] | CY 2002 No. Complaints | CY 2002 Percentage[1] | CY 2003 No. Complaints | CY 2003 Percentage[1] |
|---|---|---|---|---|---|---|
| Phone | 2,734 | 53% | 7,206 | 43% | 9,880 | 44% |
| Mail | 699 | 14% | 3,704 | 22% | 4,195 | 19% |
| Internet: | 1,299 | 25% | 3,476 | 21% | 6,192 | 28% |
| *E-mail* | *717* | *14%* | *2,014* | *12%* | *3,061* | *14%* |
| *Website* | *452* | *9%* | *1,045* | *6%* | *2,198* | *10%* |
| *Other* | *130* | *2%* | *417* | *3%* | *933* | *4%* |
| Other | 440 | 8% | 2,191 | 13% | 2,123 | 9% |
| *Total* | *5,172* | *100%* | *16,577* | 100% | *22,390* | *100%* |

[1]Percentages are based on the total number of fraud complaints where company's method of initial contact was reported by consumers age 60 and over (CY 2001=5,172; CY 2002=16,577; CY 2003=22,390). The percentage of consumers age 60 and over reporting this information is 84% in all three calendar years.

## Sentinel Fraud Top 15 Product of Service
## Consumers Age 60 and Over
*January 1 – December 31, 2003*

| Rank | Product or Service | No. of Complaints |
|---|---|---|
| 1 | Prizes\Sweepstakes\Gifts | 7,039 |
| 2 | Shop-at-Home\Catalog Sales | 2,902 |
| 3 | Internet Auction | 2,161 |
| 4 | Nigerian/Other Foreign Money Offers (not prizes) | 1,681 |
| 5 | Telephone: Pay-Per-Call\Info Services | 1,144 |
| 6 | Internet Access Services | 1,099 |
| 7 | Internet Information & Adult Services | 857 |
| 8 | Advance-Fee Loans, Credit Arrangers | 804 |
| 9 | Charitable Solicitations | 778 |
| 10 | Health Care: All | 774 |
| 11 | Lotteries\Lottery Ticket Buying Clubs | 662 |
| 12 | Computers: Equipment\Software | 647 |
| 13 | Travel\Vacations | 484 |
| 14 | Bus Opps\Franchises\Distributorships | 423 |
| 15 | Work-At-Home Plans | 367 |

## Investment-Related Scams Complaint Count

*January 1 – December 31, 2003*

| [illegible] | No. Complaints |
|---|---|
| Fraud Complaints | 2,279 |
| Fraud Complaints with Consumer Age | 1,363 |
| Age 60 and Over | 338 |
| [illegible] | [illegible] |
| [illegible] | [illegible] |
| [illegible] | [illegible] |

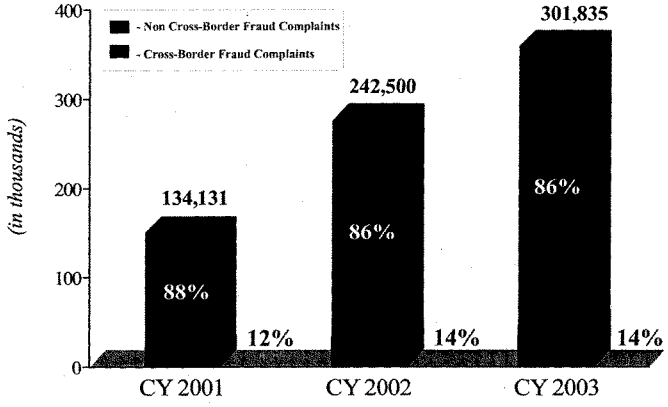
## Cross-Border Fraud Complaint Count

*January 1, 2001 – December 31, 2003*

| Calendar Year | Total No. of Fraud Complaints | Total Cross-Border Complaints | Cross-Border Complaints %[1] |
|---|---|---|---|
| 2001 | 134,131 | 16,327 | 12% |
| [illegible] | [illegible] | [illegible] | [illegible] |
| 2003 | 301,835 | 42,185 | 14% |

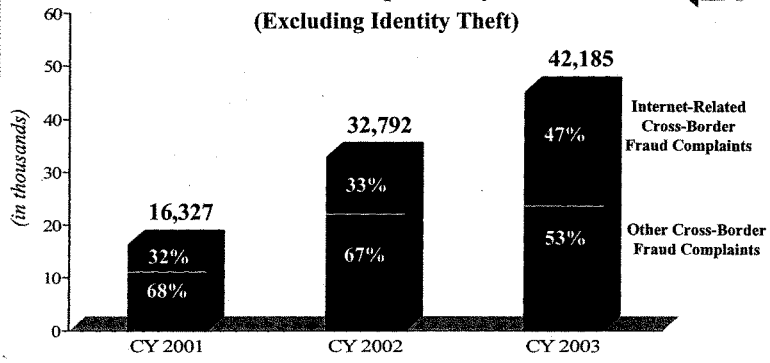
[1]Percentages are based on the total number of fraud complaints by calendar year. For the purposes of this report, a fraud complaint is "cross-border" if: (1) a U.S. consumer complained about a company located in Canada or another foreign country, (2) a Canadian consumer complained about a company located in the U.S. or another foreign country, or (3) a consumer from a foreign country complained about a company located in the U.S. or Canada. Company location is based on addresses reported by the complaining consumers and thus, understates the number of cross-border complaints. In some instances the company address provided by the consumer may actually be a mail drop rather than the physical location of the company, and in other cases, the consumer does not know whether the location is in the U.S. or abroad.

## Sentinel Fraud Complaints by Calendar Year[1]
### (Excluding Identity Theft)




[1]Percentages are based on the total number of Consumer Sentinel fraud complaints by calendar year.

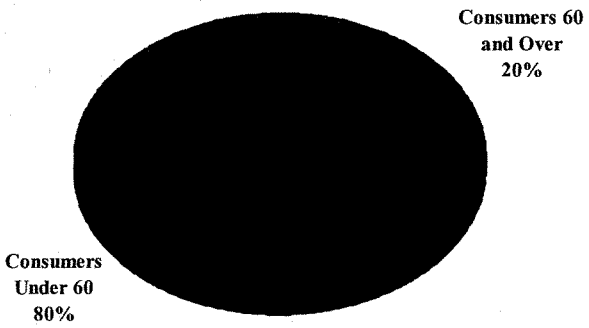
## Cross-Border Fraud Complaints by Calendar Year[2]
### (Excluding Identity Theft)




[2]Percentages are based on the total number of Consumer Sentinel cross-border fraud complaints by calendar year.

## Consumer Age Distribution for Cross-Border Fraud Complaints[1]

*January 1 – December 31, 2003*




[1]Percentages are based on 32,306 cross-border fraud complaints where consumers reported their age for calendar year 2003. Consumers reported their age in 77% of all cross-border fraud complaints during calendar year 2003.

Note: As of July 1, 2002, persons age 60 and over made up approximately 16.4% of the U.S. population. (Source: Population Division, U.S. Census Bureau, Table NA-EST2002-ASRO-01 - National Population Estimates - Characteristics, Release Date: June 18, 2003).

The CHAIRMAN. Howard, thank you very much.

Now let us turn to Tanya Solov from the Chicago Secretary of State's Office, representing the National American Securities Administrators Association. Tanya, welcome to the committee.

**STATEMENT OF TANYA SOLOV, DIRECTOR OF SECURITIES, NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, CHICAGO, IL**

Ms. SOLOV. Thank you very much. I am honored to have the opportunity to appear before you to present the States' views on protecting senior citizens against investment fraud on the Internet.

As the securities director for the State of Illinois, I interact with elderly investors who approach me at senior investor education events or call my office with complaints of fraud. My office works with criminal authorities to prosecute companies and individuals who commit crimes against seniors, and bring civil actions for injunctions and restitution. We also educate seniors through publications, videos, and seminars.

In a perfect storm, a number of significant events come together to create a devastating impact. State securities regulators are deeply concerned that a prefect storm for investment fraud is brewing, and our nation's 35 million seniors are most at risk. These days, seniors are seeking higher returns than those offered by certificates of deposit and other traditional income-generating investments. The collapse of the bubble economy and rising costs for medical insurance, prescription drugs, and basic living expenses have driven seniors to the Internet in search of alternative investments.

Most seniors do not randomly surf the Internet looking for a place to put their savings. Instead, they use the Internet as a reference tool based on a solicitation or information they have received from a friend or an associate or during a free seminar. Others may just happen upon an investment Web site, or they are recipients of unsolicited e-mail solicitation, many of them touting penny stocks, real estate, or oil and gas ventures.

The Internet has made it simple for a con artist to reach millions of potential victims at minimal cost. Investment scam artists do not have to spend money setting up boiler rooms, making phone calls, or sending mailings. They can quickly set up Web sites targeting investors with scams involving prime bank notes, viatical settlements, foreign ventures, and Ponzi schemes.

Fraud can be especially damaging for older investors because their portfolios have less time to recover. Often, older victims do not report crimes because they do not want people to know they have lost money or made an unsound investment. Also, they do not know how or where to complain.

So what can be done to combat Internet fraud? State securities regulators believe in combining enforcement efforts and financial education as the dual approach to protect investors. Seniors and all investors should always call their State securities regulator if they suspect an investment fraud. State regulators can tell the public whether or not the investment is registered in that State, whether the salesperson is licensed to do business, and whether or not there is any disciplinary history associated with the salesperson or company.

A list of regulators is available on the North American Securities Administrators Web site at www.nasaa.org.

In addition to education, State regulators are engaging in vigorous enforcement against Internet con artists. My colleague, Kansas Securities Commissioner Chris Biggs, recently announced that an investment scam promoted over the Internet resulted in a prison sentence of 44 months for the perpetrator and—fortunately in that case—a return of most of the investors' money. In that particular case, the fraudster was using the Internet and direct mail to solicit investors for a company called Venture Capital Investments. He guaranteed a high return and claimed that the investments were FDIC insured. In only 5 weeks, the fraudster raised about $85,000 from 30 investors. We brought a poster showing the Web site that was used in that particular scam. It is off to my right there. So it does look like a legitimate Web site, with frequently asked questions and other points there. That is what the seniors were directed to.

In my own State of Illinois, seniors and other investors were solicited to send small sums of money, in some instances as little as $100, to put into an entity that claimed to invest in developing countries. In the end, the scam collected over $20 million. Because the con artist in that case spent most of his investment locally, many of his purchases were seized, forfeited, and sold. The investors who applied for restitution received their money back, and the scamster and 12 other defendants were sent to prison.

State securities administrators are pursuing similar cases across the country and they are also participating in a senior outreach initiative that is designed to educate seniors to protect themselves from investment fraud. A highlight of this initiative is the Senior Investor Resource Center, which is sponsored by NASAA. The NASAA senior resource Web site includes commonsense solutions to protect assets from investment fraud and links to a variety of investor education publications and programs offered by State securities regulators and others to assist seniors. The Web site also includes a checklist of questions seniors should ask before making an investment decision, and information about the current top fraud.

In conclusion, I would like to say that investment fraud against seniors is increasing at an alarming rate. Seniors and all investors need more, not fewer, cops on the securities beat. This committee's examination of Internet fraud as it affects the growing online senior population is an important step in highlighting the problem and working toward a solution. My office and other State securities administrators will continue to play an active role in protecting seniors regardless of whether a large multimillion-dollar scam is involved or a single defrauded investor.

I thank you and your committee for allowing me the opportunity to appear today. I look forward to answering any questions that you may have.

Now in final conclusion, we do have a 30-second public service announcement that I was hoping to show regarding Internet fraud.

The CHAIRMAN. Sure. Let us hear it.

Ms. SOLOV. Thank you.

[The prepared statement of Ms. Solov follows:]

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION, INC.

NASAA

10 G Street N.E., Suite 710
Washington, DC 20002
202/737-0900
Fax: 202/783-3571
E-mail: info@nasaa.org
Web Address: http://www.nasaa.org

# TESTIMONY OF TANYA SOLOV

Illinois Securities Director
Broker-Dealer Section Chair
North American Securities Administrators Association, Inc.

Before the
Special Committee on Aging
United States Senate

"Protecting Senior Citizens Against Internet Investment Fraud"

March 23, 2004

President: Ralph A. Lambiase (Connecticut) • President-Elect: Franklin L. Widmann (New Jersey) • Secretary: Daphne D. Smith (Tennessee) • Treasurer: Craig A. Goettsch (Iowa)
Directors: Scott P. Borchert (Minnesota) • Deborah R. Bortner (Washington) • Christine A. Bruenn (Maine) • Anthony W. Patey (Newfoundland and Labrador) • S. Anthony Taggart (Utah)
Ombudsman: Robert M. Lam (Pennsylvania)

Chairman Craig, Ranking Member Breaux and Members of the Committee,

I'm Tanya Solov, Illinois Securities Director and Chair of the Broker-Dealer Section of the North American Securities Administrators Association, Inc. (NASAA).[1] I am honored to have the opportunity to appear before your Committee to present the states' views on protecting senior citizens against investment fraud on the Internet.

*Overview*

The securities administrators in your states are responsible for the licensing of firms and investment professionals, registration of certain securities offerings, examination of broker-dealers and investment advisers, investor education and the enforcement of state securities laws. Like me, ten of my colleagues are appointed by their Secretaries of State, others by their Governors, and five fall under the jurisdiction of their states' Attorneys General. We have been called the "local cops on the securities beat," and I believe that is an accurate characterization.

As the securities director for the state of Illinois, I interact with elderly investors who approach me at senior investor education seminars or call my office with complaints. My office works with criminal authorities to prosecute companies and individuals who commit crimes against seniors, and brings civil actions for injunctions, restitution and penalties against companies and individuals who commit securities fraud. We also educate seniors through publications, videos and seminars so that they may be better able to protect themselves.

The role of state securities regulators has become increasingly important as Americans rely on the securities markets to prepare for their financial futures. Today, we are indeed a "nation of investors" with over half of all American households now investing in the securities markets. And, we are a nation with a growing senior population.

*Investment Fraud Against Seniors*

In a perfect storm, a number of significant events come together to create a devastating impact. State securities regulators are deeply concerned that a perfect storm for investment fraud is brewing and our nation's 35 million seniors are most at risk. The collapse of the bubble economy, coupled with low returns on income-generating investments and rising costs for medical insurance, prescription drugs and basic living expenses, have driven seniors to seek higher returns on investments. Many view the Internet as a source for alternative investment opportunities.

---

[1] The oldest international organization devoted to investor protection, the North American Securities Administrators Association, Inc., was founded in 1919. Its membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico and Puerto Rico. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

With the Internet becoming a common part of daily life for increasing numbers of people, it should be no surprise that con artists have made cyberspace a prime hunting ground for victims. Seniors are rapidly discovering the Internet, opening up new vistas and exposing themselves to insidious new scams. A 2002 SeniorNet[2] survey on Internet use reports that 13% of senior Internet users are performing investment transactions online.

Most seniors do not surf the Internet looking for investment opportunities. Many use the Internet as a reference tool based on a solicitation, or information that they received from a friend, an associate, or during an investment seminar. Others may happen upon an investment website unintentionally, or they may be recipients of unsolicited emails touting certain investments. Older Americans who are duped via the Internet are highly intelligent and many are familiar with the Internet because they used the computer during the course of their employment. They may have utilized the computer to research and verify legitimate information, but now they are accessing professional looking websites that contain misrepresentations and fraudulent information.

The Internet has made it simple for a con artist to reach millions of potential victims at minimal cost – turning the information superhighway into a road of ruin for victims of cyber fraud. Investment scam artists don't have to spend money setting up boiler rooms, making phone calls or sending mailings. Many of the online scams that state regulators see today are merely new twists on schemes that have been fleecing offline investors for years.

We have seen the Internet used for legitimate business purposes such as direct offerings of securities through company Web sites and online brokerage services. Conversely, older investors are targeted with increasingly complex investment scams involving unregistered securities, promissory notes, charitable gift annuities, viatical settlements, and Ponzi schemes all promising inflated returns. Fraud can be especially damaging for older investors because their portfolios have less time to recover.

No one knows exactly how many older Americans are victims of investment fraud on the Internet. Often, older victims don't report crimes because they don't want people to know they have lost money, or made an unsound investment. Also, they don't know how or where to complain.

---

[2] SeniorNet is a nonprofit organization of computer-using adults, age 50 and older. SeniorNet's mission is to provide older adults education for and access to computer technologies to enhance their lives and enable them to share their knowledge and wisdom.

So what can be done to combat Internet fraud? Seniors and all investors should always call their state securities regulator if they suspect they have been the victims of investment fraud. You can find a list of regulators on the NASAA website at www.nasaa.org

State regulators can tell you whether the investment product is licensed for sale in your state and whether the salesperson has a history of wrongdoing. The best advice is to call your state securities regulator to check out any investment before investing.

*Examples of State Securities Enforcement Cases*

My colleague, Kansas Securities Commissioner Chris Biggs, recently announced that an investment scam promoted over the Internet resulted in a prison sentence of 44 months for the con artist who pled no contest to three felony counts. In that case, the fraudster was operating under the business name Free Market Brokers and Consulting and was using the Internet and direct mail to solicit investors for a company called Venture Capital Investments. He guaranteed a high return on the investments and claimed that the investments were FDIC insured, when in fact, it was a complete fraud. In only five weeks, this fraudster raised about $85,000 from 30 investors, most of whom were elderly. The Kansas securities regulators pursued this fraud and recouped much of the money for the investors.

In my own state of Illinois, seniors and other investors were solicited to send small sums of money, in some instances as little as $100, to put into an entity that claimed to invest in developing countries. In the end, the Internet con artist, who was a retired electrician in a small town in Illinois, collected over $20 million, mostly through cash sent to his home. Because he spent most of his investment locally, many of his purchases were seized, forfeited and sold. Every investor who applied for restitution received their money back and the scamster and 12 other defendants were convicted and sent to jail.

State securities regulators believe in combining enforcement efforts and financial education as the dual approach to protect investors against fraud. Earlier this year, as part of our effort to educate investors before they invest, state securities regulators identified the Top 10 scams, schemes and scandals investors are likely to face in 2004, based on prevalence and seriousness. There was a confluence of both senior investment fraud and Internet fraud included in this year's Top 10. Many of the scams, which reside on the Internet, have existed for years prior to the creation of this technology. What has given them new life, power and reach is the power of the medium.

*Senior Outreach Initiative and Senior Investor Resource Center*

State securities administrators from around the country have undertaken a Senior Outreach Initiative that is designed to educate seniors to protect themselves from investment fraud.

The Senior Outreach Initiative is:

- Promoting programs and materials developed by state securities regulators that include brochures, videos, and outreach seminars presented to organizations such as the Golden Kiwanis and Senior VFW groups.

- Developing an anti-fraud education program that utilizes volunteer/peer group educators and networks. This program is based on highly successful initiatives that have been launched in California and Ontario. The blueprint for this program will allow states securities regulators to tailor it and effectively launch it in their own jurisdictions.

- Building a clearinghouse for new and existing state programs designed specifically for Seniors. This clearinghouse can be accessed through the Senior Investor Resource Center on the NASAA website at: (www.nasaa.org/nasaa/sirc/sirc.asp)

The Senior Investor Resource Center, sponsored by NASAA and launched last fall, is designed specifically for senior audiences.

The website includes:

- A checklist of questions seniors should ask before making an investment decision;
- Common sense solutions to protect assets from investment fraud;
- Information about the current top frauds targeting seniors;
- Contact information for securities regulators in each of the 50 states, the District of Columbia, Puerto Rico, Canada, Mexico;
- An Investors Bill of Rights and Investor Fraud Awareness Quiz and;
- Links to a variety of investor education publications and programs offered by state securities regulators and others to help seniors fight investment fraud.

*Conclusion*

These are dangerous economic times for seniors. Now, more than ever, American investors need more, not fewer cops on the securities beat. This Committee's examination of Internet fraud as it affects the growing "Online" senior population is an important step in highlighting the problem and working toward a solution. My Office and other State Securities Administrators will continue to play an active role in protecting seniors whether it is a large multi-million dollar scam or a single defrauded senior. I thank the Chairman and each member of this Committee for allowing me the opportunity to appear today. I look forward to answering any questions you have and providing additional assistance to you in the future.

The CHAIRMAN. Thank you. Well done. Directly to the point.

Now let us turn to our last panelist this morning, David Jevans—I am working at it, David—the chairman of the Anti-Phishing Working Group, who is working closely with the finance and e-commerce industry on Internet crime. David, welcome to the committee.

**STATEMENT OF DAVID JEVANS, CHAIRMAN, ANTI-PHISHING WORKING GROUP, REDWOOD CITY, CA**

Mr. JEVANS. Thank you, Mr. Chairman.

I have been asked today to provide some insight on the problem of e-mail phishing, its impact on senior citizens as they get online and increase their use of the Internet.

First, I would like to start out with a definition of phishing.

The CHAIRMAN. Thank you. [Laughter.]

Mr. JEVANS. Then I will address the spelling.

The CHAIRMAN. All right.

Mr. JEVANS. "Phishing" is a hacker term for a particular type of e-mail fraud. The fraud is perpetrated by scammers and spammers. Typically, a spam is sent to random users on the Internet pretending to be from a legitimate bank, Internet service provider, e-commerce company, or Government agency. This e-mail looks exactly like an e-mail that you would expect to receive, complete with e-mail address, logo, and other branding elements of the legitimate Web site. However, the e-mail is not really from who it says it is from. It is from a fraudster. They are luring the consumer to a fake Web site in order to trick them into revealing their credit card details, bank account information, online banking password, or other personal identity information.

I would like to show some black-and-white printouts of some screen shots of phishing sites and illustrate how realistic they are.

First, you will see here an e-mail that appears to come from eBay. It has the logos. I have circled some elements here. At the top it will have a spoofed e-mail address. So it says it is from Secret Service at ebay.com. It will have the logo. It will have links that claim to be from eBay—they say go to eBay billing center. However, they are actually disguised links to some other Web site.

When you click on those links, you will be brought to a Web site that looks just like, for example in this case, the eBay site. You will see the logo, you will see requests for sensitive information, such as your user ID and password. Many times you will see other information being requested, such as your credit card information, your address, and in this case, your ATM PIN code.

Here is one that is a little more nefarious. This is from a major bank. What they have done here is, in the main window, they take you to the real bank Web site. You can see it at the top there. That is the Web site of the real bank. However, there is a pop-up window asking you to log in with your card number and your password and expiration. If you type that information into that window, it goes to a server in Russia.

Banks and e-commerce companies are not the only targets. Here is one from a major Internet service provider, AT&T. The fraudster is using their logo and claiming that you have to update your credit card information to continue to keep your account active.

Last summer, the FBI termed phishing the hottest and most troubling new scam on the Internet. Indeed, reports of phishing attacks jumped over 400 percent during the 2003 Christmas holiday season, according to the most recent analysis by the Anti-Phishing Working Group. Worse, the increasing realism of these phishing messages, including logos and professionally designed forms for entering credit card information and bank account data, have made them ever more successful. The average positive response rate is between 1 and 5 percent for the people who receive them.

Phishing attacks are also increasing in frequency, scope, and sophistication. Recently, Citigroup, Lloyds TSB, Barclays Bank have all been subject to phishing attacks that spoofed their identities in pursuit of customer account, debit and credit card data. Within the last year, Wachovia Bank, Bank of America, US Bank, Bank of Montreal, Westpac Bank, and ANZ Bank of Australia have all been hit by phishing scams. Although financial service firms were obvious initial targets for phishing attacks, adept identity thieves have expanded their phishing operations to exploit a number of Internet consumer brands and Government agencies, including Yahoo!, eBay, PayPal, Monster.com, Bestbuy.com, Microsoft MSN, and even the FDIC.

The term "phishing" comes from the analogy that Internet scammers are using e-mail lures to fish for passwords and financial data from the sea of Internet users. Now, it is spelled with a ph instead of an f. Ph is a common hacker replacement for an f, and it is a nod to the original hacking, really, from the early 1970's known as phone phreaking. In fact, it is the origin of a lot ph-spelling used in many hacker pseudonyms and hacker organizations.

Phishing scams are of particular concern to the senior community. A recent survey by Nielsen/NetRatings indicates that those 65 and older are the fastest-growing group online, and they are increasing their presence on the Internet by 25 percent in 2003. These consumers are new to the Internet and, as such, are not educated about the dangers of phishing fraud.

Another significant demographic fact is that persons over the age of 50 control at least 70 percent of the nation's household net worth. It is estimated that the elderly will control approximately $10 trillion in assets within the next 10 years. Because phishing is a financial crime, seniors make particularly appealing targets. Fortunately, it is still difficult for phishers to target seniors specifically. However, there are e-mail data bases available on the Internet that are used by spammers for sending spam. These data bases often do categorize e-mail addresses by the interests of each consumer. Thus, it is feasible for a phisher to obtain or derive a list of e-mail addresses that could be used for more targeted attacks.

The senior population make appealing targets, and should be particularly careful of phishing attacks because they potentially have the most to lose. If a banking or investment account were to be compromised, the phisher would have access to significant assets. Also, if personal identity information, such as a Social Security number, is obtained by a phisher, the criminal can apply for bank loans or credit cards using the identity of the consumer. Because many seniors have good credit ratings and more sizable as-

sets, the phishers will be able to obtain larger loans and credit limits.

I recommend that consumers exercise caution when they receive any e-mail that requests personal identity or financial information. Any e-mail that takes you to a Web site that requests such information should also be inspected carefully. Because the sender can be faked in e-mail, consumers cannot trust that an e-mail was sent to them from their bank, ISP, or e-commerce site just by looking at the From field of the e-mail.

I would like to share a few recommendations for consumers to protect themselves.

First, examine the Web address or URL of any Web page you are taken to by an e-mail. If that Web page does not match the Web address you are used to, be very suspicious.

In my experience, I have almost never seen a legitimate reason for a Web site to ask for a Social Security number. Any site that asks for this information should be regarded with great suspicion.

Similarly, there is no reason for any site to request your ATM PIN or password. Any site that requests this is fraudulent.

If you receive an e-mail purporting to be from a company, bank, or even Government agency that you do not do business with, and this e-mail requests personal identity or financial information, be extremely suspicious. There have been instances in recent months where e-mails were sent out purporting to be from the FDIC or Regulations.gov Government agencies. These e-mails have used scare tactics to frighten consumers into divulging personal information.

Consumers should always use anti-virus software and keep it up to date. You should also do weekly scans of your computer for viruses or Trojans.

My last tip is consumers should also keep their computer software up-to-date with the latest updates from Microsoft. There are new updates issued by Microsoft every week or two, and they are usually to fix new security problems that phishers could exploit.

The Anti-Phishing Working Group has been organized to develop an acceptable solution to e-mail phishing scams. This is an organization of over 180 members from financial institutions, law enforcement, ISPs, and the e-commerce community. I am the chairman of the organization, and my day job is senior vice president at Tumbleweed Communications, a vendor of secure e-mail and anti-spam technology.

The Anti-Phishing Working Group has established the www.antiphishing.org Web site as a repository of information about phishing. The site contains a news feed of articles about phishing as well as an ever-expanding archive of known phishing e-mails and Web sites. Proposed technology solutions, lists of vendors and Government agencies who can help combat phishing are also listed on the site.

The working group members are exploring technology solutions to allow businesses to authenticate or digitally sign their e-mails to consumers. These techniques would allow consumers to determine that the sender of an e-mail was really who it purported to be. There are other technology solutions being tested, including detection and scanning services.

Members of the Anti-Phishing Working Group are working together to develop educational messages and best practices for consumers and companies. The working group is working with other organizations that are looking to combat Internet fraud, including the Bankers Information Technology Secretariat and the Information Technology Association of America. Consumers should also be aware that the Federal Trade Commission and the U.S. Department of Justice have advisory bulletins and other information available on their Web sites.

That concludes my remarks. Thank you.

[The prepared statement of Mr. Jevans follows:]

**Testimony of David Jevans**

## PHISHING EMAIL FRAUD

Greetings Commissioners:

I have been asked today to provide insight on the problem of email "phishing" fraud, and its impact on senior citizens as they get online and increase their use of the Internet. First, I'd like to start out with a definition of "phishing".

Phishing is a hacker term for a particular type of email fraud. This fraud is perpetrated by email scammers and spammers. Typically, a spam email is sent to random users of the Internet, pretending to be from a legitimate bank, Internet Service Provider ("ISP"), e-commerce company or government agency. This email looks exactly like an email that you would expect to receive, complete with the email address, logo and other branding elements of the legitimate website.

However, the email is not really from who it says it's from. It's from a fraudster who is luring the consumer to a fake website, in order to trick them into revealing their credit card details, bank account information, online banking password or other personal identity information.

[ Here I would like to show some screenshots of phishing sites. illustrating how realistic they are.]

Last summer, the FBI termed phishing "the hottest, and most troubling, new scam on the Internet." Indeed, reports of email phishing attacks jumped over 400 percent during the 2003 Christmas holiday season, according to the most recent analysis by the Anti-Phishing Working Group. Worse, the increasing realism of the phishing messages - including logos and professionally designed forms for entering credit card information and bank account data - have made them ever more successful, with an average positive response rate of between 1 and 5 percent of those who receive them.

Phishing attacks are increasing in frequency, scope and sophistication. Recently, Citigroup, Lloyds TSB and Barclays Bank have been subjected to phishing attacks that spoofed their identities in pursuit of customer's account, debit and credit card data. Within the last year, Wachovia, Bank of America, US Bank, Bank of Montreal, Westpac Bank, and the ANZ Bank of Australia, have been hit by phishing scams. Although financial services firms were obvious initial targets for phishing attacks, adept identity theives have expanded their phishing operations to exploit a number of Internet consumer brands and government agencies including Yahoo!, eBay, Paypal, Monster.com, Bestbuy.com, Microsoft MSN and even the FDIC.

The term "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users. The term was coined in the 1996 timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. The first mention on the Internet of phishing is on the alt.2600 hacker newsgroup in January 1996. however the term may have been used even earlier in the printed edition of the hacker newsletter "2600".

"Ph" is a common hacker replacement for "f", and is a nod to the original form of hacking in the early 1970s, known as "phone phreaking". This is in fact the origin of a lot of the "ph" spelling in many hacker pseudonyms and hacker organizations.

By 1996, hacked accounts were called "phish", and by 1997, there is evidence that "phish" were actually being traded between hackers as a form of currency. For example, people would trade 10 working AOL phish for a piece of hacking software that they needed.

Over the years, phishing attacks grew from simply stealing AOL dialup accounts into a more sinister criminal enterprise. Phishing attacks now target users of online banking, electronic payment services and online e-commerce sites.

Phishing scams are of particular concern to the Senior community. A recent survey by Nielsen/NetRatings indicates that those 65 and older are the fastest growing group online,

increasing their presence on the Internet by 25% in 2003. These consumers are new to the Internet, as such, are not educated about the new dangers of phishing fraud.

Another significant demographic fact is that persons over the age of 50 control at least 70% of the nation's household net worth. It is estimated that the elderly will control approximately $10 trillion in assets within the next 10 years. Because phishing is a financial crime, seniors make particularly appealing targets. Fortunately, it is still difficult for phishers to target seniors specifically, however there are email databases available on the Internet that are used by spammers for sending spam. These databases often do categorize email addresses by the interests of each consumer. They get these categorizations by harvesting email addresses from newsgroups and mailing lists that cater to particular interests. Thus it is feasible for a phisher to obtain or derive a list of email addresses that could be used for more targeted attacks. However, they do not need to do so, as a spam-like broadcast of a phishing email to millions of email addresses will reach many seniors.

The senior population make appealing targets, and should be particularly careful of phishing attacks, because they potentially have the most to lose. If a banking or investment account were to be compromised, a phisher would have access to significant assets. Also, if personal identity information such as a social security number is obtained by a phisher, then the criminal can apply for bank loans or credit cards using the identity of the consumer. Because many seniors have good credit ratings and more sizeable assets, the phishers will be able to obtain larger loans and credit limits.

The challenge for seniors, and in fact for most consumers, is that phishing attacks are increasingly sophisticated, and difficult to discern from legitimate emails. I recommend that consumers exercise caution when they receive any email that requests personal identity or financial information, or that takes you to a website that requests such information. Because the sender can be faked in email, consumers cannot trust that an email was sent to them from their bank, ISP or an e-commerce site just by looking at the "From:" field in the email.

Here are some recommendations for consumers to protect themselves:

- You should examine the web address (or "URL") of any web page that you are taken to by an email. If that web page address does not match the web address that you are used to, be very suspicious.

- In my experience, I have almost never seen a legitimate reason for a web site to ask for a Social Security Number. Any site or email that asks for this information should be regarded with great suspicion.

- Similarly, there is no reason for any site to request your ATM PIN. Any site that requests this is fraudulent.

- If you receive an email purporting to be from a company, bank, or even government agency that you do not do business with, and this email requests personal identity or financial information, be extremely suspicious. There have been instances in recent months where emails were sent out purporting to be from the FDIC or from Regulations.gov government agencies. These emails have used scare tactics to frighten consumers into divulging personal information. Such phishing emails suggest that a consumer's bank account has been compromised by crooks or terrorists, and the consumer should enter their bank account information for verification, or risk having their bank account frozen.

- Consumers should use anti-virus software and keep it up to date. Use the software not only to protect from inbound viruses, but also to do a weekly scan of your hard disk for any viruses or Trojans that may have slipped through the anti-virus filter.

- Keep your computer's software up to date with the latest updates from Microsoft. There are new updates issued by Microsoft every week or two, and they are mostly to fix newly discovered security problems that phishers could exploit.

The "Anti-Phishing Working Group" has been organized to develop an acceptable solution to email phishing scams. This is an organization of over 180 members from financial institutions, ecommerce providers, ISPs, law enforcement agencies and software vendors. I am the Chairman of the organization, and a Senior Vice President at

Tumbleweed Communications, a vendor of secure email and anti-spam technology. The goal of the Anti-Phishing Working Group is to provide resources, technology, vision and expertise to facilitate the rapid deployment of a solution to email phishing scams.

The Anti-Phishing Working Group has established the www.Antiphishing.org website as a repository of information about phishing. The site contains a news feed of articles about phishing, as well as an ever-expanding archive of known phishing attack emails and websites. Proposed technical solutions, lists of vendors and government agencies who can help combat phishing are also listed.

The working group members are exploring technology solutions to allow businesses to authenticate, or digitally sign, their emails to their customers. These techniques would allow consumers to determine that the sender of an email was really who they purported to be. Other technology solutions being tested include detection and scanning services to monitor attacks as they happen.

Members of the Anti-Phishing working group are working together to develop educational messages and best practices for consumers and companies. The Anti-Phishing working group is working with other organizations that are working on combating Internet fraud including the Bankers Information Technology Secretariat (BITS) and the Information Technology Association of America (ITAA). Consumers should also be aware that the Federal Trade Commission (FTC) and U.S. Department of Justice (DOJ) have advisory bulletins and other information available on their websites.

The CHAIRMAN. Well, David, thank you for that testimony and that explanation. In fact, as you were showing that first eBay lure, I guess, I am having these quick memory flashbacks. Literally on Saturday of this past weekend, I was at my son-in-law's home, who makes his living servicing the Internet for a provider, and we were accessing eBay to look at some activity on eBay and he went by one of those, saying, Oh, that is a phony, and just passed it by. I never asked why.

I now know. He knew, obviously, because he spends a good deal of his professional life there. But it is fascinating that you would pull that one up today, because that was literally one that he had on his computer or had been sent to him, and he passed it by very quickly, saying, That is a phony. I never questioned him. But I find that very curious. Thank you.

Dave, let us come back to you. You mentioned Senate Bill 153, that has already passed the Senate. Hearings are going on today. Could you reiterate for us the importance of having Federal statutes that impose stiff penalties on these types of crimes that are embodied within Senate Bill 153?

Mr. NAHMIAS. Well, as I mentioned, the existing penalties are, in most cases, pretty good, both the underlying Federal sentencing guidelines and enhancements that can be used where the criminals target particularly vulnerable victims or people particularly susceptible to crimes.

In the case of identify theft, our concern is the way the guidelines work. Someone who commits identity theft, which is almost always part of another crime, they get your identity to use your credit card information or commit some other fraud. Under the guidelines those crimes merge and there is no additional penalty in most cases for the identity theft portion of that crime, even though it tends to create a different kind of harm to the victim. We are supporting this bill that has passed the Senate, which would impose a—in most cases a 2-year minimum additional penalty on top of the underlying penalty for the crime committed with the stolen identity information, and thereby serve as a deterrent to people who would potentially commit crimes with identity theft information.

In the case of a crime that relates to terrorism, the additional penalty would be 5 years, and we believe that that would be an important enhancement to the overall scheme of punishing people who commit these kinds of crimes.

The CHAIRMAN. Can you tell us more about the involvement of organized criminal networks in financial fraud cases in general, and I should say, who are the major players and where do they originate from as you now know it?

Mr. NAHMIAS. Some of my fellow panelists may be able to speak to this as well, but——

The CHAIRMAN. In all of these questions, as the person asked pauses at the end, if you have additional information to put into it, please do so for the record. Thank you.

Mr. NAHMIAS. I think in our experience our prosecution of Internet fraud cases indicate, you see everything from individuals like the person who testified on your first panel, to organized groups, both domestic and international. We are not aware of any specific

cases in which traditional organized crime groups such as La Cosa Nostra or motorcycle gangs have been particularly involved in these kinds of Internet fraud schemes, although much of the activity does involve groups of people acting together. The only other thing I would say is Internet crime is an extension of traditional fraud schemes as Mr. Maxwell was talking about. It is the same schemes we have seen for years using this particularly——

The CHAIRMAN. Just a new vehicle?

Mr. NAHMIAS. A new vehicle which is a very valuable vehicle for criminals because it is so anonymous, easy to do over distances and very hard for law enforcement to crack into because the data is often fleeting, and unless you get onto it quickly it may be gone.

So as traditional organized crime groups see how these new tools can be used, there is not reason to think that they will not try to use them as they have other tools in the past.

Mr. MAXWELL. I would agree with that, Mr. Chairman. The only additional information I would throw out is because most of the situations we have had here in the United States are primarily one individual or two. Child exploitation sometimes involves a couple or two or three people, but in most fraud schemes we have had it has been one individual or two with the exception of those coming from abroad.

We have some concerns about some of them coming from the former Eastern Bloc via the Internet. It was mentioned I think earlier there was a site going back to Russia. Those are the concerns because they present such a challenge in terms of prosecuting and enforcement, and those are the difficulties we are facing now.

We are exploring strategies, primarily with Canada. There is a cross-border crime forum, as you are probably very well aware of, which we have an Internet telemarketing group, and we are part of that along with our colleagues in the other agencies and FTC. That shows a lot of promise, but it has been going on for 10 years and we still have a lot more to accomplish, but that will be a proving ground for what may come in the future.

The CHAIRMAN. Anyone else? Yes, David.

Mr. JEVANS. Mr. Chairman, in the last 7 months we have seen phishing sites from being largely hosted in the United States to being hosted primarily in Eastern Europe as well as in Asia. This makes it very difficult to tear the sites down. Instead of being able to tear it down in a few hours, maybe half a day, it can take up to 160 hours, basically a week, to tear the sites down.

The other thing we have seen is that these do tend to be groups of two or three people who largely meet in online chat rooms. They are basically working from home, and it will be a spammer, a fraudster and maybe a virus writer.

Ms. SOLOV. If I may also, from the State perspective, the fraud, for example, that I mentioned from the State of Illinois, that started as a one-man operation by a retired electrician in a very small town in Illinois. Then as he made money, he drew other people in to assist and ultimately there were, I believe, 18 defendants in that case, most of whom were convicted. That is what we are seeing at the State level.

But very commonly, with regard to investment fraud, individuals are invited to a free seminar where they get coffee and donuts and

an explanation about, for example, some great real estate venture. Then they are encouraged to go to a website to "verify" that all of the information presented at the seminar is in fact true and accurate. We find that that is often happening with senior citizens who attend seminars and then use the Internet as a verification tool.

The CHAIRMAN. You said something I think very important, and I watched it in older people who I know and some within my family, who never were heavy stock investors, but they accumulated substantial amounts of money and they had a lot of CDs, and the CD market, as you know, is no place to be today because of the interest being paid, and so they are really impacted by a decline in revenue that they had adjusted to because of their CDs, and they are out looking and asking, and I have parents, my wife has parents, who ask us those questions. Where do we go to get a better return on our investment? I think they must be phenomenally susceptible to the kind of thing you have spoken to.

Ms. SOLOV. Yes, and that is a line that is very commonly used. The con artists say, "You are not really making any money on the certificate of deposit. In fact, you are probably losing money ultimately, so here are some alternative investment opportunities."

The CHAIRMAN. I mentioned something in my testimony—and maybe, Dave, you can respond to it, or certainly any of you who wish. A few weeks ago we held hearings in this room on the implementation of the soon-to-be prescription drug discount card, and there is a lot of work being done to stand up websites where they can go online and look at different opportunities, go online to look at difference in pricing. We are asking seniors to become much more knowledgeable in accessing the Internet for the purpose of accessing knowledge on how to buy drugs and all of that type of thing, and this will accelerate. Have any of you done any thinking about the potential fraud that is going on in that area, and has the Department of Justice taken notice of this as a real possibility?

Mr. NAHMIAS. Senator, that is a very good question, and actually the FDA, the Food and Drug Administration is the agency on the front line of that issue of ensuring that the drugs are safe. Although the Department of Justice and our law enforcement regulatory partners need to provide a supporting role in terms of the FDA's enforcement effort, that issue is being examined by a task force in the administration. The Conference Report for the Medicare Modernization Act required the Secretary of HHS to examine the issue of drug importation and look at limits on resources and legal authorities. I know both within the Department of Justice and within the administration, that is an area that we are looking at because of the concern that on the one hand we are expanding the funding in that area and directing people to the Internet as a source of information; on the other hand we realize that where there is money and where there is the Internet, there is a potential for criminal activity. So I think that is an area that we are concerned about and we are trying to get on the front end of.

The CHAIRMAN. You are right to assume there is going to be a substantial amount of money flowing in that respect.

Anyone else wish to comment on that?

Mr. MAXWELL. It presents a little bit of a problem from my agency's standpoint. I have had several discussions with our counter-

parts at Food and Drug Office of Criminal Investigation, and also I met with our counsel's office, and I guess our jurisdiction really was somewhat limited to the fraud end of those types of promotions. If they can enhance some of the other provisions in terms of either under a DEA schedule or some other type of avenue for us, we could probably have more reason to be involved. We certainly do welcome and we recognize the problem. I remember there were hearings on this two or 3 years ago and that created quite a stir.

The CHAIRMAN. Lawrence, let us stay with you. We have all talked about seniors and their fixed incomes, but also we talked about the money they have and the money they seek to invest, and they have tremendous buying power as a class of citizen in our country, and they give a lot. They are very charity minded.

Are you able to tell us if any charity monies given by seniors has found its way into the hands of suspected terrorist organizations?

Mr. MAXWELL. That is the question of the hour, actually, because we had inspectors assigned to Green Quest, which was the first initiative back under Treasury, and it has morphed into some different names now, but with a focus primarily on that type of activity. What we saw was some limited cases where it could clearly be drawn, and of course, you have read some of the headlines where certain individuals were charged, I think in Illinois was one I read about where they were dismissed later because there was not enough to show that tie into terrorism.

It is clearly a concern from a security standpoint if nothing else, but also from a fraud standpoint, people being victimized based on their good nature. We have a lot of types of these things happening, like right after 9/11 we would see them crop up. After any calamity generally you will see these things emerge.

It is just very difficult to identify them quickly enough to take action before people are hurt. So the sooner we hear, the better always.

The CHAIRMAN. David, is a false website, let us say in a post-9/11 event where monies are being asked for for charitable purposes and it is a fraud, is that considered phishing?

Mr. JEVANS. That is typically not considered phishing unless somebody is sending out spam e-mails to pull people into one that may be replicating a legitimate one. So you may see things where there is a legitimate site out there collecting monies and someone sets up a fake one, and they pull people in that way definitely.

The CHAIRMAN. Go ahead, please.

Mr. BEALES. If I could just add to that. What we see most often in fraudulent charitable solicitations is badge fraud, where the——

The CHAIRMAN. It is what?

Mr. BEALES. Badge fraud. The appeal is to help the local police or fire fighters or some local connection like that. We have brought those kinds of cases and worked with State and local partners in those kinds of matters, but what we have—that is where we most frequently have seen the fraudulent kinds of solicitations.

The CHAIRMAN. Howard, let us stay with you. You mention in your testimony seniors continue to be hit by telephone fraud 44 percent of the time. Is it true that phone use for senior scams is decreasing as the use of the Internet is increasing?

Mr. BEALES. It certainly is in our complaints. We are seeing more and more Internet and less and less telephone. That is very much the trend, but it is hard to say how much of that is real and how much of that is the nature of complaints. Complaints are easier online, so for people who are online and where the contact is online, they may be more likely to file a complaint and that would change the relative proportions.

There is clearly still a lot of telemarketing fraud out there, and we are bringing numerous telemarketing cases that go after those problems.

The CHAIRMAN. Do you know if Internet fraud now exceeds the U.S. Mail service as a means of scamming people over 60?

Mr. BEALES. It certainly does as a means of the first contact in our complaints, and again, with the same caveat, that it is hard to tell how much of that is real and how much of it is complaints.

The CHAIRMAN. President Bush signed anti-spam legislation last year. How is the fight against spam going at this moment?

Mr. BEALES. The fight against spam is going to be a long and difficult one. There is no single or easy solution unfortunately. We have brought already more than 60 cases under the FTC Act, challenging fraudulent and deceptive spam. We have numerous other investigations in the pipeline and will continue to devote a lot of resources to it.

We are engaged in rulemakings to implement parts of that statute. We just published a broad advance notice of proposed rulemaking on the kinds of rules that might be necessary. We are also working closely with the criminal authorities to try to develop cases that may be appropriate for criminal prosecution under Can Spam. There is progress, and but it is slow and it is going to take time.

Mr. JEVANS. Mr. Chairman.

The CHAIRMAN. Yes?

Mr. JEVANS. We have noticed that there has been some decrease in spam to the companies that launched major lawsuits a week or so ago. That would be Microsoft, AOL. Earthlink and Yahoo came together and launched quite a number of lawsuits. AOL has come out and said they have seen a decrease in the amount of spam. However, the overall amount of the spam on the Internet, which we are measuring on a daily basis, has not decreased.

The CHAIRMAN. Is it increasing?

Mr. JEVANS. It continues to increase, and it may be just that it is moving away from those big entities who have a lot of legal muscle, and just moving out to everybody else.

The CHAIRMAN. Thank you.

Tanya, would you highlight for us the top three investment schemes that seniors seem to be drawn to and why?

Ms. SOLOV. The top one is probably I would say the scheme where investors are asked to invest in a company that is just going public, and generally these are "startup companies" that usually deal with either technology or medicine. They are companies that are touting that they have the cure for cancer or for AIDS or other ailments. So that is probably the top scam that we are seeing.

Second, we are seeing a tremendous number of scams involving real estate ventures. The public has heard that one segment of the economy that continues to grow and is doing really well is real es-

tate. So the con artists have set up shops indicating that they are investing in real estate ventured.

Third, I would say prime bank notes or foreign investments. Again, senior have heard the term—and other investors too—one must diversify. So they are encouraged to invest in foreign investments, foreign currencies and at companies that are allegedly investing in developing countries.

The CHAIRMAN. David, who is liable if a consumer falls for a phishing attack and their information is stolen and misused?

Mr. JEVANS. Typically if it is a credit card that has been stolen, generally the consumer is protected under Regulation Z, and the bank typically or the merchant will be liable on the Internet, if it is using an Internet merchant, it would be the merchant. However, if a consumer's bank account information is——

The CHAIRMAN. But right now we just heard Dave say that the theft of the identity is not punishable as much as what you use the identify for; is that correct?

Mr. NAHMIAS. They are separate crimes and you can charge someone, but under the sentencing guidelines currently they merge for sentencing purposes so there is no additional penalty, and frankly, prosecutors often do not charge them because you have to prove more and you do not get any bank for your buck.

The Chairman. I see.

Go ahead, David.

Mr. JEVANS. Typically people are prosecuted under wire fraud, mail fraud, bank fraud. So if it is a credit card, the consumer is usually OK. It is usually the merchant who is liable. If it is a bank account that has been basically broached, legally in the United States it would be consumer who is liable because they have divulged their password to someone who is not the bank. However, fortunately, banks will make consumers whole, and in the rare case it happens, they will usually reimburse them.

If a Social Security number is taken and loans are taken out against the consumer, if they can prove fraud they can usually get restitution, but that can be a long drawn-put process.

The CHAIRMAN. David, I am going to ask you this last question, and you all may want to respond to it. We recently, at least within the last year and a half or two, saw a movie with Tom Hanks and Leonardo DiCaprio, in which Leonardo was the ultimate check-writing artist and ID scam artist. True story. He was ultimately caught by the FBI and their Check Fraud Division, and ultimately used by them to take down other check writers. You have just heard Mr. Groover this morning offer some suggestions. Obviously, he was talented enough at the time to take a lot of money out of ID theft and credit cards. You are apprehending people who are obviously very talented at what they do to access and to develop fraudulent documents and materials on the Internet. Are you using them? Are they willing to come forward after caught? Is their information and their knowledge a usable commodity? Do you solicit from them for information blocking the kind of scams that go forward, or are they simply stuck in a Federal pen and left there?

Mr. JEVANS. Regrettably, most of them have not been caught, particularly in the phishing side of things which is technologically advanced. We have established some communication with people.

The ones who have been caught mostly have been amateurs. The more technical ones, there have been dialogs. We understand what they are doing. There appears to be correlation between what they are doing and virus writers. As we all know, catching virus writers is extremely difficult. There are rewards out of hundreds of thousands of dollars and nobody has been really caught yet.

I thought that Mr. Groover had some very good points and some of those could definitely help.

The CHAIRMAN. Did you take notes?

Mr. JEVANS. Absolutely, absolutely.

The CHAIRMAN. Can you imagine going back to the office and saying, "I have just gotten this information from a convicted felon?"

Mr. JEVANS. I will be. [Laughter.]

The CHAIRMAN. All right.

Mr. JEVANS. I thought his idea about a pass key to your credit reporting information was definitely a good one and would not require wholesale re-engineering of that system. However, you do have the vulnerability that if you type that into a fraudulent website, that person has got it, so there are some technical things that need to be worked out there.

The CHAIRMAN. Anyone else wish to react to that last comment or question? Howard?

Mr. BEALES. Senator, I think there is a delicate balance that the Congress worried very much about in re-authorizing the Fair Credit Reporting Act at the end of last year, between security of credit information, which is clearly important, and ease of access to credit on behalf of consumers who need credit. There really are some difficult tradeoffs there. I think there are a great many Americans who do not know they have a credit report, let alone able to remember the pass key that they would need to get into it——

The CHAIRMAN. Until they are told——

Mr. BEALES. That is bad.

Mr. MAXWELL. Senator.

The CHAIRMAN. Yes.

Mr. MAXWELL. To get right to the heart of what you said earlier, I did not have the pleasure of meeting Mr. DiCaprio, but I did meet Mr. Frank Abagnale, who was what the movie was based on.

The CHAIRMAN. Yes.

Mr. MAXWELL. We invited him to speak at one of our fraud training symposiums, and a fascinating individual, as you would expect. He mentioned that he does one venture a year for the Federal Government to pay back what he had done to the country, because I engaged him in conversation and she shared that with me.

We have videotaped telemarketing, people convicted of telemarketing cases, investment schemes, and we use them in our training effort. If David will forgive me, we also invite them to the defense bar sometimes, to come and help train our agents, so it is very valuable. Yes, I took notes as well.

The CHAIRMAN. The criminal mind is usually a pretty bright mind.

Mr. MAXWELL. Yes, very much so.

Mr. NAHMIAS. I would agree. We learn a lot from the people we catch. Usually our preference is both to have them incarcerated and to learn from them, rather than other alternates, but the Fed-

eral sentencing guideline system is set up to create great incentives for people to cooperate with the Government. The other thing I would say, is while I think Mr. Groover had some good ideas, I was pleased that some of the ideas he has such as interagency coordination to collect complaints are already in effect.

The CHAIRMAN. I did see you smiling once there when he made that comment.

Mr. NAHMIAS. It is nice to know that we are ahead of the criminals on some things, and really a lot of the credit for that goes to the FTC.

The CHAIRMAN. Tanya, gentlemen, thank you all very much for your testimony today, as we continue to try to stay on top of this rapidly evolving issue. I oftentimes tell this story, and I will conclude with it.

I have a mother-in-law who lives in a retirement community in Tucson. Five years ago there was a lovely pool room in that retirement community, and I walked by there with my father-in-law, and nobody was using it. Two pool tables, the lights were out. I said, "Nobody plays pool here?" He said, "Not really." At that time, and still today, my wife is much better on the Internet and with a computer than I, and she was teaching my father-in-law and mother-in-law to gain access to the Internet. They said, "You ought to do this for the rest on this living group." That evolved into the taking out of the pool room and the putting in of a computer room. I think there are 12 terminals there now.

I was down there recently. My father-in-law has since passed away, but my mother-in-law is still very active. Walked by there at about 10 o'clock one night in a community in where the average age is probably 78 to 80, and there were five people in there, talking to their grandchildren and their kids, and on eBay, so the world is changing very rapidly for that senior community. They were slow to come to the Internet, but they are now coming very rapidly, as I mentioned, and we are now encouraging them to go there, and certainly my generation of baby boomers, they are all going to be pretty computer literate when they get to that age. So what we do here now and the foundational work we do to catch the fraud and the criminal that will access them through the Internet, is I hope productive work.

I thank you all very much for being with us this morning. The Special Committee will stand adjourned.

[Whereupon, at 12:09 p.m., the Special Committee was adjourned.]

○