AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 107–728

IDENTITY THEFT: THE NATION'S FASTEST GROWING CRIME WAVE HITS SENIORS

HEARING

BEFORE THE

SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

WASHINGTON, DC

JULY 18, 2002

Serial No. 107–30

Printed for the use of the Special Committee on Aging

U.S. GOVERNMENT PRINTING OFFICE

82–327 PDF WASHINGTON : 2002

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

JOHN B. BREAUX, Louisiana, *Chairman*

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
JEAN CARNAHAN, Missouri

LARRY CRAIG, Idaho, *Ranking Member*
CONRAD BURNS, Montana
RICHARD SHELBY, Alabama
RICK SANTORUM, Pennsylvania
SUSAN COLLINS, Maine
MIKE ENZI, Wyoming
TIM HUTCHINSON, Arkansas
JOHN ENSIGN, Nevada
CHUCK HAGEL, Nebraska
GORDON SMITH, Oregon

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

CONTENTS

	Page
Opening Statement of Senator Larry E. Craig	1
Statement of Senator Susan Collins	2

PANEL I

Lieutenant Colonel (Retired) John T. Stevens, Jr., Upper Marlboro, MD	4
Alice S. Fisher, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice, Washington, DC	11
James G. Huse, Jr., Inspector General, Office of Inspector General, Social Security Administration, Washington, DC	24
Howard Beales, Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, DC	34
Douglas Coombs, Deputy Special Agent in Charge, Financial Crimes Division, United States Secret Service, Washington, DC	59

PANEL II

Mari J. Frank, Esq., Privacy and Identity Theft Consultant, Laguna Niguel, CA	80
Boris F. Melnikoff, Consultant to the Regional President, American Bankers Association (ABA), Atlanta, GA	100
Stuart K. Pratt, Vice President, Government Relations, Consumer Data Industry Association, Washington, DC	113
Dennis Carlton, Director of Washington Operations, International Biometric Group, LLC, Washington, DC	137

IDENTITY THEFT: THE NATION'S FASTEST GROWING CRIME WAVE HITS SENIORS

THURSDAY, JULY 18, 2002

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

The committee convened, pursuant to notice, at 9:30 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Larry E. Craig, presiding.

Present: Senators Craig, Carper, and Collins.

OPENING STATEMENT OF SENATOR LARRY CRAIG

Senator CRAIG. Good morning, everyone. Thank you for being here. Let me welcome all of you and our witnesses to today's hearing here before the Special Committee on Aging.

First and foremost, I want to thank Senator John Breaux of Louisiana, who chairs this committee, for the opportunity to address this most important issue. I think Senator Breaux will attempt to join us later on, as some of our other colleagues on the Special Committee may also.

But I do believe, and I think all of us in Congress believe, that it is important to address the identity theft issue and the tragedy that this besets upon our nation's seniors. Identity theft is the nation's fastest growing white-collar crime. It is estimated that over 700,000 Americans become victims of identity theft each year. Several thousand of those victims are senior citizens, who are uniquely vulnerable to this insidious crime.

As you may recall, in June of last year, I held a hearing on elder abuse. We heard testimony about crimes committed against our most vulnerable senior citizens. Today, you will hear about a different type of crime that is on the rise.

Our nation's seniors spend a lifetime working hard to maintain their independence and develop a legacy that they and their families can be proud of. With one fraudulent transaction, identity theft can strip away a senior's independence, sense of security, and dignity. Identity theft can destroy legacies and reputations, leading to depression and despair.

To effectively fight this crime, it is critical that law enforcement and the private sector work together. For example, Idaho law encourages financial institutions to report suspected instances of elder financial crime to local authorities. Banks in Idaho, in cooperation with State agencies, provide training to their employees on how to identify and prevent financial crime targeting the elderly, including identity theft. Idaho is only one of five States to im-

plement such a program. I say "only." It should be 50 States of the Nation aggressively pursuing this relationship between the private and the public sector.

We also need to determine how existing State and Federal efforts might be enhanced to promote cooperative approaches in resolving these very complex cases. Penalties should be enhanced when these acts ruin the lives of our most vulnerable citizens. Existing Federal resources can and should be targeted toward providing more technical training in the identification and prosecution of identity theft.

I commend the Department of Justice and other key Federal agencies here today in their efforts to combat this crime. I support Attorney General Ashcroft's current aggressive nationwide sweep to pursue and prosecute individuals engaged in identity theft, including those targeting the elderly.

Finally, I would like to announce my cosponsorship of S. 2541, which lengthens prison sentences for those who would perpetrate the insidious and destructive crime of identity theft.

I look forward to the testimony from our witnesses today. I also view this as an opportunity to build a record that my colleagues will look at and consider as they encourage their States, both private and public sector law enforcement and crime prevention, to participate in fighting identity theft.

With that, let me invite our first panel before us. We have a cross-section of those involved in law enforcement and the public sector and those who have experienced this kind of situation.

Let me first introduce to the committee and to the room Lieutenant Colonel, Retired, John Stevens of Upper Marlboro, MD. John is one of those who I understand has experienced this kind of problem in his life, so John, we look forward to your testimony. Please proceed.

Excuse me. We will hold you off for just a second. I have just been joined by Susan Collins of Maine, a Senator, a member of this committee, and let me allow her to make her opening statement, John, before we proceed with your testimony. Thank you.

Susan, welcome.

STATEMENT OF SENATOR SUSAN COLLINS

Senator Collins. Thank you very much, Senator.

Today, the Special Committee on Aging will explore the impact of identity theft on our nation's seniors. Identity theft is an insidious crime. Unlike many types of fraud, in which victims are enticed by deceptive claims or lured by deals that are too good to be true, identity theft can occur when a victim is simply engaging in everyday activities, or in other cases, by unwittingly providing confidential personal information to the wrong party. Identity thieves use their victims' personal identifiers and financial information to commit bank and credit card fraud, insurance fraud, and a host of other criminal acts.

While anyone can be the victim of identity fraud, seniors are among the most vulnerable. The number of seniors who have become the victims of identity theft is growing rapidly. Reported incidents among those aged 60 years and older skyrocketed by a staggering 218 percent between the year 2000 and 2001, and these fig-

ures are likely to only continue to grow as America's elderly population increases.

Some of the very achievements that seniors have worked for their whole lives contribute to this vulnerability. For example, their often excellent credit ratings make the elderly a particularly appealing target for identity theft. Many seniors have strong credit ratings earned over the years by faithfully paying their bills on time. This good credit is abused by identity thieves who take out loans, sign leases, or open bank or credit card accounts and run up bills in the elderly person's name. In a very short amount of time, a lifetime's worth of solid credit, along with the pride and dignity it brings, can be ruined.

Other aspects of seniors' lives also make them more vulnerable to the tactics used by identity thieves. Some seniors are simply unaware of the threat. They are unaware that perhaps by engaging in transactions on the Internet that they may be vulnerable to identity theft. Consequently, not only are they unable to take simple preventive measures, but they also may be unaware that their identity has even been stolen for some period of time.

Moreover, fraudulent telemarketers take advantage of seniors who live alone by seeming to offer friendship when their true purpose is to pump the elderly person for personal information.

As the Chairman of the Permanent Subcommittee on Investigations during my first 4 years in the Senate, I held numerous hearings on consumer fraud. Two years ago, I chaired a PSI hearing that examined the increasing availability of false education and credentials, such as drivers' licenses, birth certificates, and Social Security cards, over the Internet. One of the subcommittee's findings was that false identification facilitates a host of other crimes, ranging from underage drinking to credit card and bank theft to identity theft.

One witness who used false identification documents to aid in stealing others' identities testified that not only was he able to gather personal information about his victims online, but he also was able to gather all the false identification documents he needed online, as well. Another individual used false identification, apparently obtained from a website operator, to perpetrate identity theft and a host of financial crimes, eventually racking up debts of $35,000 in the victims' name.

In December 2000, the Internet False Identification Prevention Act of 2000, which I authored, became law, but I still think there is a great deal more that we need to do. One of the things that we can do is to increase public awareness about this problem, and that is why I am pleased that the Senate recently passed legislation, the National Fraud Against Senior Citizens Awareness Week, which I hope will lead to activities like this.

I also want to thank Senator Craig for his leadership in holding this hearing this morning. Thank you, Mr. Chairman.

Senator CRAIG. Senator Collins, thank you, and thank you for your leadership in this area. It is a matter of not only seniors understanding the risks involved, but trying to plug the holes and most assuredly going after those with effective prosecution, so thank you again.

Now, let me turn to our panel, and once again, Lieutenant Colonel, Retired, John Stevens from Maryland. Welcome before the committee and please proceed. We would ask all of you to stay with our 5-minute rule. Your full statements that you provided for the committee will become a part of the committee record. Thank you.

STATEMENT OF LIEUTENANT COLONEL (RETIRED) JOHN T. STEVENS, JR., UPPER MARLBORO, MD

Colonel STEVENS. Good morning, Senator Craig, Senator Collins. My wife, who is sitting directly behind me, and I wish to thank this committee for your concern of the effects of identity theft on the senior citizens of this country.

I am 74-years old and my wife is 3 years younger. We are rapidly approaching our 49th wedding anniversary. We are still fighting the identity theft battle that began in 1997. Our battle now is not with the impostors that used our Social Security numbers to open 33 fraud accounts worth $113,000, but with the creditors, credit bureaus, and third party collection agencies.

By working 12 to 14 hours a day, paying $6,000 in attorney fees, and spending a small fortune in phone bills, we cleared the fraud accounts from our credit reports in about a year. However, this was only temporary. They would reappear, in our credit reports, from the same creditor or a third party collection agency. The life of these fraud accounts was extended by the cavalier attitude of the credit bureaus and the profit motive of creditors in failing to establish policies and procedures that would prevent this.

This recycling of fraud accounts and other personal fraud data has been going on now for over 4 years, with no end in sight. We never know what we are going to find in our credit reports. We are tired of getting threatening letters and phone calls from collection agencies. We are tired of constantly correcting the fraud accounts and erroneous data that keeps appearing in our credit reports. We are tired of having to pay cash for purchases, that would normally be financed, because of the fraud, data that keeps reappearing in our credit reports. We are tired of creditors and collection agencies trying to extort money from us, with the help of the credit bureaus on known fraud accounts. We want creditors and credit bureaus to be held fully accountable for the time, misery and expense involved in correcting their errors.

We are not victims of this crime. We are targets. As a target, we will fight back, take evasive action, and employ countermeasures against the enemy. I have already survived two wars and intend to fight to win this one. My wife and I are warriors. We intend to fight back for as long as it takes to overcome the horror of this crime and regain control of our lives.

Identity theft is only possible with the full cooperation of the three major participants. In our opinion, the impostor, the creditor, and the credit bureaus are all co-conspirators and equally guilty of identity theft.

Last year, we contacted an attorney in Louisiana to take action against the creditors and credit bureaus in an effort to stop their harassment and attempted extortion. We found out that there is a 2-year time limit on taking legal action. Of course, this only bene-

fits the co-conspirators who are responsible for this crime and not those affected by it. This time limit should be removed.

The credit bureaus now sell protection from identity theft. Equifax "Credit Watch" and Experian's "Credit Manager" will alert you to significant changes in your credit report and send you copies to check the accuracy of the data. Protecting the integrity and ensuring the accuracy of information contained in a credit report should be a normal part of their operation and not just available to those willing to pay them for "protection."

My wife and I continuously warn people about identity theft and how to fight it when it happens. We also warn about other related scams, against the elderly, such as automatically raising auto insurance rates at age 70, rejected medical insurance claims that are only paid upon resubmission, being billed for magazine subscription renewals you did not order and threats to ruin your credit if you do not pay, telemarketers trying to sell you unwanted merchandise, merchants who demand your Social Security number for routine purchases, and pharmacies that routinely short your pill count on prescription drugs.

We advise others to "opt out" of the exchange of personal information by banks and other businesses. This practice needs to be changed to "opt in" only.

How much longer must we put up with having our credit ruined and being harassed and insulted by creditors and collection agencies? Why must our personal information be distributed to others who use it to harass us with unwanted sales pitches and junk mail? Why must we continuously correct errors in our credit reports caused by the incompetence and greed of others?

We want our lives back. Enough is enough. My wife and I would like to enjoy what time we have left to be together in this world. Our feelings can simply be expressed by quoting a line from the movie "Network." "I am mad as hell and I am not going to take it anymore." It is time to throw the money changers out of the temple.

Senator CRAIG. John, thank you. That is powerful testimony. We appreciate it.

[The prepared statement of Colonel Stevens follows:]

UNITED STATES SENATE
SPECIAL COMMITTEE ON AGING
John T. Stevens, Jr.
July 18, 2002

My wife and I wish to thank this committee for their concern over how Identity Theft can affect the senior citizens of this country. I am 74 years old and my wife is three years younger. We have been married for almost 49 years. We can tell you first hand that fighting identity theft is not a very pleasant experience. Once it happens it can consume your life for years. We are still fighting it after five years. Its life is extended by the cavalier attitude of the creditors and the credit bureaus and their reluctance to establish policies and procedures that will reduce its occurrence. This is especially evident when these policies conflict with the convenience of opening an account or the money generated from their accounts. They have even refused to prosecute the persons, who commit this crime, when they are identified. We hope that by speaking here today we can bring you some understanding of this crime and how the creditors and the credit bureaus perpetuate it through their inaction, indifference and profit first attitude. Two years ago we heard testimony before the House Social Security Subcommittee about all the fabulous safeguards the credit bureaus were going to implement to protect the consumer from identity theft. We have not experienced any of these changes. When we testified before a committee of the House of Delegates in Maryland for the third time, we heard from the credit bureaus, insurance companies and government agencies how everything would come to a halt if the social security number could not be used to identify a person or exchange data. It would be inconvenient for them to use other means to verify the identity of a person. I wonder how businesses and government agencies managed to exist before 1935. The first social security cards issued had a warning, "NOT FOR IDENTIFICATION". Again the bill did not pass. Once again we were sacrificed on the altar of profit and convenience. Our nightmare began in March 1997 with a phone call from (then) Nations Bank. They demanded payments on a Jeep Cherokee financed through them last year. I told them that I do not have a Jeep Cherokee. I faxed them a copy of my drivers license and they faxed me a copy of the application. The only thing correct on the application was my first and last name and social security number. Nations Bank in Wichita Falls, Texas approved the application showing a local address in Texas. Although I have lived in Maryland since 1966, the Texas address was accepted and the application approved. We immediately requested copies of our credit reports. The results? A total of 33 fraud accounts with a monetary value of $113,000. There were a total of five automobiles purchased. What is ironic is that this had been going on for about a year and we were not aware of it until after the Nations Bank phone call. This was only one of five fraud accounts opened in Texas with Nations Bank. I already had a checking account with them opened in 1950 when I first went on active duty in the Air Force. My bank statements have come to my address in Maryland since I was stationed at the Pentagon in 1966. The date of birth shown on the applications showed that my social security number, which they were using, was issued before they were born. Nobody bothered to compare the application data with that given in a 45-year-old active checking account showing a different address and age. The fraud address and employment data was accepted by the credit bureau and became a part of my credit report. It still keeps reappearing in my credit reports although I have corrected it many times.

Since 1997 my wife and I have been going through the hell of attempting to clear the fraud accounts and correct the fraud data that keep reappearing in our credit reports. Why is it so easy for fraud accounts and data to be put in our credit reports and so difficult to have it removed? We have been yelled at, insulted, and humiliated by creditors and third party collection agencies and ignored by credit bureaus as we attempted to straighten out this mess. We were accused of being dead beats, of not paying "your" bills and defaulting on "your" loans. We have been denied credit and been forced to pay cash for major purchases that would have normally been financed. Our Maryland home has been under surveillance and my Ford Bronco almost towed, by Nations Bank, when trying to re-possess the Jeep Cherokee they had financed in Texas. My wife currently has a court default judgment against her for furniture bought and delivered to an address in Texas. We obtained a copy of the application from Greens Furniture Company in Wichita Falls, Texas. Even though personal information was missing or inaccurate, the application for credit was approved, after a favorable credit report from the credit bureau based on a correct social security number. Our attorney called the judge in Wichata Falls, Texas to have it removed. We are still waiting for a response from her. Our social security numbers are accessible at any military base connected to the network of DOD computers that issue ID cards and service the DEERS program. Until just recently, we had to put our social security number on a check used to make purchases in a Base Exchange or Commissary. This is no longer required, thanks to the efforts of the House Social Security Subcommittee and Chairman Clay Shaw.

I am a retired Air Force Officer. While on active duty, any breach in personal integrity or fiscal responsibility, even writing a bad check, would have ended my career or chance of promotion. After an automobile accident forced me to retire in 1971, I was employed as a physicist by The Johns Hopkins University Applied Physics Laboratory. I was trusted by both government and industry to have the integrity, experience and knowledge to analyze, test and evaluate advanced and complex weapon systems. Any breach of personal or fiscal responsibility would have affected my security clearance and ended my employment. After retiring from Johns Hopkins University, my wife and I were looking forward to moving to South Carolina to be near my Mother and closer to our children and grandchildren. Unfortunately we found that our credit rating, due to the influx of all the fraud accounts, put us in the high-risk, high interest rate category for obtaining a loan to buy a house. We still haven't made it to South Carolina. My Mother died in May last year at the age of 97.

By working twelve to fourteen hours a day, hiring an attorney, using the internet to locate creditors and incurring astronomical phone bills, we managed to clear most of the fraud accounts from our credit reports in about a year. Or, so we thought. When a creditor was finally located, our attorney would send them an affidavit disclaiming any knowledge of the account. The creditor would notify the credit bureaus to remove the fraud account from our records. Usually in two to three months this same account would be placed back into our credit report through a third party collection agency. It is difficult to trace the origin of a third party collection agency account. We were able to trace them by looking for the heavily disguised original account number appearing in their newly assigned

account numbers. A letter to the credit bureau would sometimes clear this account from our report when we were able to link it to a previously cleared fraud account. However, it would usually reappear in our report after three to four months. If the third party collection agency cleared the account, it would end up with another collection agency or, in some cases, with the same collection agency and back into our credit report. So far we have dealt with fourteen third party collection agencies. They are not pleasant people to deal with. They are rude, nasty, insulting and determined that this is "your debt and "you" will pay it, or else we will ruin your credit rating. We refused to be intimidated by their threats and they ruined our credit rating. One of the worst was Household Bank. They opened an account over the phone and delivered an Oreck vacuum cleaner to an address in Wichita Falls, Texas. When the delinquent account appeared in my credit report I wrote a letter to the credit bureau challenging this account. After their usual 30-day investigation, Equifax stated in their report "This creditor has verified that this account information is being reported correctly". I contacted Household Bank directly. They are the most arrogant, rudest people I have ever dealt with. They were rude and insulting to my attorney and me. At first they refused to accept my sworn affidavit. Household Bank finally accepted my affidavit and this account was temporarily removed from my credit report until it reappeared through a third party collection agency. I have cleared it with this agency four times. The last credit report I received, prior to testifying before a committee of the Maryland House of Delegates, showed that it had again been returned to my report. This is only one of many cleared fraud accounts that keep reappearing in our credit reports. To paraphrase Forest Gump, "Getting a credit report is like opening a box of chocolates, you never know what you are going to get".

We have had to continuously fight fraud accounts that keep reappearing in our credit reports after they are cleared. These creditors are very persistent and determined to harass us until they make us pay, even a reduced amount, on these fraud accounts. Some people will pay them just to get rid of their constant abuse and harassment. What they are not told is that this fraud information will remain in their credit report for seven years. Paying any amount is an admission of guilt. My wife and I are concerned that these fraud accounts will show up again when our estate goes to probate. They will probably try again to extort money from us with what they know to be fraud accounts.

We tried to get assistance for our legal expenses and telephone bills through our homeowner's insurance policy. USAA replied to me, "There has been no direct physical loss to personal property; no apparent actual credit card theft forgery on accounts established by you, or issued to you. Having your credit record questioned is not a loss that would be covered in our policy contract, under the Additional Coverage provision of your policy". We had anther home insured by Armed Forces Insurance. They provided $1000 to help offset some of our expenses. Our legal expenses have exceeded $6000 plus phone bills to track down the fraud accounts. Last year we obtained the name of an attorney in Louisiana who agreed to take our case. This was the only way that we knew to stop the constant harassment and attempts to extort money from us by creditors and credit bureaus. We were blocked from taking any action because of a court decision placing a two-year time limit on taking legal action against a fraud account. Some of the accounts were two years old before we knew they existed or figured out what to do to fight them.

A time limit, to take action against those causing or contributing to this crime can only benefit the creditors and the credit bureaus, definitely not the targets of this crime. I use the word **TARGET** because the word **VICTIM** does not describe our feelings or actions taken to combat this crime. A **VICTIM** just rolls over and accepts what is happening. We consider ourselves **TARGETS** because we fight back, take evasive action and employ countermeasures against the enemy. Our **WARRIOR** instinct does not allow us to give in to the attempted extortion and constant harassment by the creditors, third party collection agencies or the incompetent data collection and false information provided and constantly re-cycled by credit bureaus. Our experience has shown that the impostor stealing your identity, the creditor, and the credit bureaus are all co-conspirators and equally guilty of identity theft.

Help has finally arrived to help us combat identity theft. The credit bureaus have devised a program to combat the crime they helped to create. Equifax has now has a program called "Equifax Credit Watch". For $69.95 a year they will help you monitor, manage and protect your credit. They will alert you whenever a credit account is opened in your name. For $12.95 you can get your credit report and FICO credit score. For $9.00 you can receive a complete copy of your credit history. With this report you can "Catch and correct inaccuracies that may have negative, long-term effects on your credit history". Experian has a service called "Credit Manager". For $79.95 a year they will provide unlimited access to your credit report, and e-mail alerts of significant changes in your report. For $9.00 they will send you a credit report to "verify your personal credit information". Trans-Union will send you one free report a year, if you live in Maryland or several other states, and charge $5.00 for additional copies. In other words they all accept fraud data that is different from other long-term data, use it to ruin your credit, and charge you for protection to prevent it. What happened to the fraud alert requiring a creditor to confirm with you that you are the person applying for credit and other obvious changes to long-term data that could easily spot a fraud application? All of this should be a normal part of the credit bureau procedure. Now they charge you for this protection. You have to pay them to get a copy of a report with your information that they sell to others, to insure that the data collected on you, without your permission or knowledge, is correct. Protecting the integrity and insuring the accuracy of the information contained in a credit report should be a normal part of their operation and not an extra charge only for those willing to pay for "protection".

Citizens our age are not only vulnerable to identity theft but to other scams that take advantage of our age and trusting nature. Our experience has taught us to be alert at all times to protect ourselves and avoid the possible consequences of providing seemingly innocent information to anyone who asks for or demands it. The Medicare card contains your social security number. These cards are copied by medical personnel and left in unsecured storage containers with your medical records. The social security number is the beginning point of identity theft. Telemarketers continuously try to get personnel information about you and to sell you unwanted material or sell the information to other scam artists. We use our caller ID and only answer the phone between the third and fourth ring. Telemarketers usually hand up after the second or third ring. Don't forget to block or erase those "Cookies" that web sites write to your hard disk. Insurance

companies raise the rate on automobile insurance after age 70. Magazines will send a bill for a subscription that you did not order or want to renew. I had to write Readers Digest when they threatened my Mother with a collection agency if she did not send the payment for a subscription she did not renew. They withdrew their threat when they could not produce an authorization from her to renew the subscription. Never pay a bill until you are sure it is legitimate. Why do we always have to "Opt out" of having your name and personal information distributed by a company or bank? Why shouldn't it only be to "Opt in" if you wish to be hassled by everyone trying to sell you something. My wife and I continuously warn people about identity theft and how to avoid telemarketing annoyances and possible scams. We tell them to call the Federal Trade Commission at 1-877-IDTHEFT and request their booklet and get a councilor if you need help. If a store or business wants to write your social security number on a check or charge slip, walk away and leave the purchases on the counter. When Alltel required us to put our social security number on a cell phone application, we bought the service from another company. It is our policy NEVER to buy anything over the phone when you did not initiate the call. Don't be polite to them. Just hang up. Never buy anything from a door-to-door salesman or a contractor "who just happens to be in the neighborhood". Medical insurance companies routinely disapprove a bill on the first submission. I had to correspond with Medicare for over a year before they finally paid the claims for my Mother and stepfather. She had already paid over $10000 in bills, thinking that Medicare did not cover them. Medicare supplemental insurance sometimes has to be routinely resubmitted before the bill is paid. I still have a dental insurance claim, which is almost a year old that has been resubmitted three times. By not paying claims on time, the insurance companies can cause a medical bill to be sent to a third party collection agency and ruin a person's credit

It seems that we are fighting a never-ending battle against Identity Theft. We have observed that any legislation that is proposed, which restricts the operation of a creditor or credit bureau, is doomed to failure. Any bill that limits the use of the social security number as the primary means of identification or linking databases, does not pass. We, the consumers, are limited in our legal options against creditors and other businesses that cause and perpetuate identity theft problems through their negligence. We are forced into a two-year limit on taking legal steps on identity theft or required to accept arbitration through an arbitrator selected by the creditor. We have watched as bills, which would help us, are defeated or never come up for a vote. Is it because they would make banks and credit card companies accountable and responsible for their actions? We can only hope that more people will follow our example. We refuse to do business with anyone who wants our social security number without a legitimate reason. We throw away junk mail and never talk to telemarketers. I delete, without reading, the "cookie" generated e-mail that I get on my computer. I also block and delete "cookies". Door to door salesman are not welcome at our house. In short, the banks and other businesses may distribute and share information about us against our wishes, consent or knowledge, but they are wasting their money. We will not respond or spend one dime on the products or services they are hoping to sell us. Our feelings can be simply expressed by quoting a line from the movie "Network", "We're mad as hell and we're not going to take it anymore". It's time to throw Moneychangers out of the Temple!

Senator CRAIG. Now, let me introduce to the committee Alice Fisher, Deputy Associate Attorney General, Criminal Division, U.S. Department of Justice. Alice, thank you for joining us.

STATEMENT OF ALICE S. FISHER, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Ms. FISHER. Thank you, Senator Craig and Senator Collins, and thanks for giving me the opportunity to testify about identity theft in senior citizens and our efforts at the Department of Justice.

As you noted, identity theft is not only a serious crime but one of the fastest growing means of fraud in the United States. Criminals steal personal identification information each year in the thousands to commit crimes ranging from bank and credit card fraud to international terrorism. Americans lose money, houses, their good credit, et cetera. It goes on.

These crimes may work particular hardships, financial and emotional, on the elderly. The elderly may have a harder time recovering financially. They may be less able to withstand the emotional toll from what you have to go through to recover your identity, as we just heard.

Perhaps because identity theft does not usually involve face-to-face contact between criminal and victim, we do not see identity thieves as a group appear to be specifically targeting senior citizens. There is no doubt, however, that some criminals plan and carry out identity theft fraud knowing that their victims are senior citizens. Let me give you some examples of Federal prosecutions involving identity theft and seniors.

In a case now under Federal indictment, the defendants and others allegedly worked together to identify houses in the metropolitan Detroit area that were owned free and clear by the elderly people. The defendants would steal the identity of the true owners of the houses. Then they would strip the equity out of the house by faking refinancing without the owners' knowledge or consent. Sometimes they would fake a straw sale of the home.

In another case, a defendant in North Carolina stole mail from senior citizens throughout the State, used the identification information to produce fake drivers' licenses and counterfeit checks, then used the licenses and checks to withdraw the seniors' life savings out of bank accounts. I am pleased to report that one such defendant was just sentenced to over 5 years in prison.

In another Federal prosecution, the defendant took a job as a live-in companion for an elderly woman. After the elderly woman was hospitalized, the defendant obtained and used credit cards in her name, stealing thousands of dollars. Here, too, this defendant received significant jail time.

It goes without saying that identity thefts such as these are extremely harmful to the victims, especially senior citizens. Once an identity thief has obtained access to the victim's bank or financial accounts, the victim may suffer significant financial losses and considerable emotional distress.

In a recent Federal prosecution in Texas, one of the victims was an 80-year-old military woman whose checkbook had been stolen from her car. After the criminals had drained thousands of dollars

from her bank account, her doctor had to treat her for a stress disorder she experienced as a direct result of the crime.

The Department of Justice regards identity theft as serious criminal violation that requires a coordinated response from all levels of law enforcement, Federal, State, and local. The Department has, therefore, undertaken a three-pronged approach to identity theft.

First, the Department is vigorously pursuing identity theft prosecutions across the country. Most recently, in May, the Department conducted a nationwide sweep of Federal prosecutions targeting identity theft. In that sweep, the Department brought 73 criminal prosecutions against 135 individuals in 24 districts. The offenses charged included cases in which defendants bilked Americans of millions of dollars, preyed on the elderly, and destroyed the credit worthiness of hard-working families.

Second, the Department is pursuing additional legislation to address the most serious cases of identity theft and to provide greater protection to the public through enhanced criminal penalties, and I am pleased that, Senator Craig, you are cosponsoring this bill introduced by Senator Feinstein, S. 2541, which would create a new crime of aggravated identity theft. This new class of identity theft is defined by the nature and seriousness of the crimes committed through the use of another's identity. Individuals found guilty of identity theft under this proposed bill will receive an additional 2 years' imprisonment over and above for their sentence for the underlying offense, or an additional 5 years' imprisonment where the underlying offense is terrorism-related.

Third, the Department recognizes the importance of educating law enforcement and the general public about identity theft. Too many people, even criminal justice professionals, do not fully understand what identity theft is or how it can affect their lives and assets. As a result, the Department is sponsoring or directly supporting a number of approaches to identity theft education and prevention.

Thank you, Senator Craig and Senator Collins. I ask that the full text of my written remarks be entered in the record.

Senator CRAIG. They will be. Thank you very much for that testimony.

[The prepared statement of Ms. Fisher follows:]

Statement of Alice S. Fisher
Deputy Assistant Attorney General
Criminal Division
Before the
Special Committee on Aging
United States Senate

July 18, 2002

Mr. Chairman and Members of the Committee, thank you for the opportunity to come here today to testify about identity theft and senior citizens. As the Attorney General recently stated, identity theft is one of the fastest growing crimes in the United States. An estimated 500,000 to 700,000 Americans each year have their identity stolen, according to the Privacy Rights Clearinghouse, and many more Americans are victimized by the crimes that identity theft facilitates. These crimes range from bank and credit-card fraud to international terrorism.

Identity theft is an especially difficult crime because the criminal and the victim of the identity theft may never have any personal contact. Identity thieves obtain valuable personal data – such as Social Security numbers, credit-card numbers and expiration dates, and bank account numbers – from a growing variety of sources. Some criminals may use high-tech methods, such as hacking and "spoofing" of websites (i.e., creating fraudulent websites that look like legitimate sites), to conduct their identity thefts through computers and the

Internet. In a federal case recently indicted in the Eastern District of New York, *United States v. McNeese,* the defendant was the administrator of a computer database containing personnel records for approximately 60,000 employees of the Prudential Insurance Company. The defendant allegedly stole the database for which he was responsible, and proceeded to solicit bids for the sale of that information over the Internet. Fortunately, one of the bidders was a detective assigned to the New York Electronic Crimes Task Force, who used an undercover identity to communicate with the defendant, leading to his arrest.

Many identity thieves, however, continue to rely on low-tech means of obtaining other people's forms of identification. These low-tech approaches range from breaking into cars or stealing from mailboxes to "dumpster diving" – that is, rummaging through dumpsters or trash bins to find bank or credit-card statements or "preapproved" credit-card materials that the recipients did not shred or tear up. In one case that a person reported last week to the Department of Justice, a driver employed at the same company as the victim simply took the victim's Social Security number off a company document and proceeded to apply for multiple credit cards in the victim's name.

Perhaps because identity theft in general does not require direct contact between criminal and victim, identity thieves as a group do not appear to be specifically targeting senior citizens in particular. There is no doubt, however, that in certain situations, criminals plan and carry out identity theft and fraud knowing full well that their victims are senior citizens. Here are some examples of federal prosecutions involving identity theft and seniors:

- In a case now under federal indictment in the Eastern District of Michigan, *United States v. Billings*, the defendants and others allegedly worked together to identify houses in the metropolitan Detroit area that were owned free and clear by elderly people. The defendants would allegedly steal the identity of the true owner. They would then strip the equity out of the houses without the owner's knowledge or consent. The defendants allegedly accomplished this by faking a "re-financing" of the property (where they would withdraw equity and obtain a mortgage in the owner's name, and then default on the mortgage). Alternatively, they would fake a "straw sale" of the home. (In these cases they would forge a quit claim from the true owner to a second subject and then "sell" the home to a third subject, who would obtain a mortgage on the property.

The second subject obtained the proceeds of the "sale", and the third subject defaulted on the mortgage.)

- In a completed federal prosecution in the Eastern District of North Carolina, *United States v. Hooks*, the defendant stole mail from senior citizens throughout North Carolina, used the biographical information contained in the stolen mail to produce fake drivers' licenses and counterfeit checks, and then used the licenses and checks to withdraw the citizens' life savings out of their bank accounts. To produce the licenses, the defendant had obtained an official North Carolina Department of Motor Vehicles license machine. (He later claimed that he purchased the DMV machine on eBay.) In this case, which the United States Secret Service investigated, the loss resulting from the defendant's criminal conduct was $177,472.63. The defendant ultimately pleaded guilty to mail theft, production of false identification documents, and use of false identification, and was sentenced on November 1, 2000, to 63 months imprisonment. The conviction was upheld by the U.S. Court of Appeals for the Fourth Circuit in 2001.
- In another federal prosecution in the Eastern District of North Carolina, *United States v. Robinson*, the defendant took a job as a live-in companion

for an elderly woman. After the elderly woman was hospitalized, the defendant obtained and used credit cards in the elderly woman's name, stealing $47,051.35. In this case, which the United States Secret Service also investigated, the defendant pled guilty to access device fraud and production of false checks, and was sentenced in May 2000 to 31 months imprisonment.

There is no doubt that identity theft can create significant hardships for its victims. Once an identity thief has obtained access to the victim's bank or financial accounts, the victim may suffer significant financial losses and considerable emotional distress. In a 2001 federal prosecution in the Northern District of Texas, *United States v. Lake*, one of the victims was an 80-year-old military widow whose checkbook had been stolen from her vehicle. After the criminals had drained thousands of dollars from her bank account, her physician states that he had to treat her for high stress she experienced as a result of the identity theft.

In some cases, long periods of time may go by before the identity theft victim realizes that he or she has been targeted. In a federal prosecution in the

District of Arizona, *United States v. Hooper*, the defendant, a Canadian citizen, pleaded guilty on April 5, 2002 to fraudulent use of a Social Security number. The defendant admitted that since 1982 she had been using the Social Security number of a naturalized U.S. citizen for the purpose of concealing her true identity and obtaining credit. The victim had had her Social Security card and other identification documents stolen in Canada in 1982. Because the victim was originally a Canadian citizen and was averse to using credit for purchases, the defendant's fraud went undetected for 20 years. During that period, the defendant, while using the victim's Social Security number, got an Arizona driver's license, filed for bankruptcy in Oklahoma, and was arrested.

Identity theft victims, beyond any direct financial losses they may suffer, often encounter unanticipated additional burdens. For many identity theft victims, the process of contacting credit bureaus and creditors and trying to restore their good names and credit can be extremely frustrating. While creditors may want victims to produce evidence of the identity theft, such as a police report, many police officers may not know that identity theft is a crime in their state and may be disinclined to take a police report if they believe that the

actual frauds resulting from the identity theft took place outside their jurisdiction.

The Department of Justice regards identity theft as a serious criminal violation that requires a coordinated response from all levels of law enforcement --federal, state, and local. The Department has therefore undertaken a three-pronged approach to identity theft. First, the Department is vigorously pursuing identity theft prosecutions across the country. Most recently, in May 2002, the Department conducted a nationwide "sweep" of federal prosecutions targeting identity theft. In that sweep, the Department brought 73 criminal prosecutions against 135 individuals in 24 districts.

Second, the Department is pursuing additional legislation to address the most serious cases of identity theft and to provide greater protection to the public, through enhanced criminal penalties. S. 2541, which Senator Feinstein introduced with bipartisan sponsorship on May 22nd, would create a new crime of aggravated identity theft. This new class of identity theft is defined by the nature and seriousness of the crimes committed through the use of another's identity. Under the provisions of S. 2541, individuals found guilty of

aggravated identity theft will receive an additional two years imprisonment over and above their sentences for the underlying offense, or an additional five years imprisonment where the underlying offense is terrorism-related. S. 2541 would also enhance the current identity theft statute, section 1028, by prohibiting not just the transfer or use of another's identity information, but also possession of such information in conjunction with the requisite criminal intent. In addition, the maximum penalties for identity theft are increased and a higher maximum penalty is included for identity theft used to facilitate acts of domestic terrorism.

Third, the Department recognizes the importance of educating law enforcement and the general public about identity theft. Too many people, even criminal justice professionals, do not fully understand what identity theft is or how it can affect their lives and assets. As a result, the Department is sponsoring or directly supporting a number of approaches to identity theft education and prevention.

With respect to law enforcement, the Department has integrated training about identity theft into many of the curricula for federal prosecutors at the

Department's National Advocacy Center. Basic courses on white-collar crime and cybercrime, as well as advanced training on Internet fraud and other types of major fraud, now include training modules on identity theft. In addition, the Department has enthusiastically cosponsored a series of law enforcement training seminars about identity theft with the Federal Trade Commission and the United States Secret Service. To date, these joint training seminars, which have been held in Washington, D.C., Chicago, Des Moines, and San Francisco, have provided much-needed training to more than four hundred local, state, and federal law enforcement officers. Another of these training seminars is set for August 2002 in Dallas. The Department, the FTC, and the Secret Service are now actively discussing plans to expand these seminars to other areas of the country.

One of the elements of our training seminars on identity theft involves the Identity Theft Data Clearinghouse of the Federal Trade Commission's Consumer Sentinel database. The Clearinghouse offers investigators secure online access to an extensive database of more than 189,000 complaints as of the end of June 2002 about identity theft. Because the Department regards Consumer Sentinel as an invaluable resource in investigating identity theft cases, our training explains

what kinds of complaint data are available in Consumer Sentinel and how investigators and prosecutors can get access to Consumer Sentinel to search the Data Clearinghouse.

In addition, the Secret Service and the International Association of Chiefs of Police are now exploring the development of a "roll call" video that would be made available to police departments throughout the United States. This roll call video would allow police departments to provide their officers at roll calls with a concise explanation of identity theft and its significance as a criminal problem. More police departments need to understand the problem of identity theft and the importance of responding to identity theft victims by taking police reports. We are hopeful that this project can encourage many more officers to assist victims and pursue identity theft cases in their states.

With respect to the general public, the Department also supports a variety of education and prevention efforts. For example, the Department has a website on identity theft that explains the crime, how it can be committed, and what people should do if they think they have become identity theft victims. Very recently, the Department has added to its website an identity theft quiz for

consumers. This quiz, which can be found at www.usdoj.gov, provides consumers with a handy checklist of what they can do to reduce the risks of becoming identity theft victims, and how to report if they think they have become victims. Finally, the Department works closely with the FTC in its ongoing public education efforts about identity theft. We believe that the FTC has done an excellent job of public outreach and prevention on this subject, and are happy to provide continuing support of its efforts.

Mr. Chairman, that concludes my prepared remarks. I will be happy to respond to any questions that you or other members of the Committee may have.

* * *

Senator CRAIG. Now, let me turn to James Huse, Inspector General of the Social Security Administration here in Washington. Jim, please proceed.

STATEMENT OF JAMES G. HUSE, JR., INSPECTOR GENERAL, OFFICE OF INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, WASHINGTON, DC

Mr. HUSE. Thank you, Senator Craig and Senator Collins, for holding this important hearing this morning on identity theft and America's senior citizens.

Criminals do not steal the identities of the elderly so they can pretend to be old and wise. They do it because senior citizens are more likely than most of us to have significant assets, savings, investments, paid-up mortgages, good credit, and Federal entitlement checks. People over age 50 control at least 70 percent of the nation's household net worth. They are also easier and safer to rob. Some are less sure of themselves, more trusting, and less aware of simple precautions. Anybody can steal candy from a baby, but criminals know our older Americans have money for the taking and they do not cry out loud.

Identity theft is an enabling crime, one that permits criminals to commit other crimes more effectively. In most cases, identity theft begins with the misuse of a Social Security number, the SSN. No aspect of my mission of protecting Social Security programs from fraud, waste, and abuse is more important than our oversight of the use and misuse of the SSN.

There is an almost infinite variety to these cases. Thieves are finding houses owned by the elderly, as Ms. Fisher testified, assuming the identities of the true owners and stripping the equity out of their houses without their owners' knowledge or consent.

In San Diego, a man who had been a fugitive felon for 17 years with four prior felony convictions, including prison escape, used a 70-year-old South Dakota woman's SSN to create 33 stolen or fictitious identities. He also took out credit cards and loans under these assumed identities while receiving Social Security benefits under three of his identities.

A Virginia man working under a senior citizen's SSN while collecting disability benefits under his own number obtained over $24,000 worth of loans and credit for goods and services. The older man's credit was damaged and his retirement benefits were interfered with because of the earnings posted to his records at SSA.

Many elderly individuals who trust the Social Security Administration are victims of scams promising more information or additional Social Security benefits. Such victims have been tricked into parting with their Social Security numbers and other personal identifiers, simply assuming that SSA never responded to their request for information.

Yesterday's Washington Post had this story by Dan Oldenburg on a "do not call" registry scam that victimized the elderly. The caller asks for personal information, a bank account or credit card number, supposedly to verify if you are on a list, but it was a scam. These, of course, are used and sold for illegal purposes.

Congress has enacted helpful legislation to treat the disease of identity theft in its later stages. The ability to prevent identity

theft is even more essential. While we cannot return the SSN to its original limited function, we must take workable steps to limit both its use and the expansion of its use.

First and foremost, the time has come to make the difficult determinations as to those uses that are appropriate and necessary and those that are merely convenient. The SSN has become a de facto national identifier and its daily use has, in many instances, become a luxury we can no longer afford. The availability of SSNs on public documents and over the Internet, for example, must come to a stop.

Congress should consider requiring the cross-verification of SSNs through both governmental and private sector systems of records. Only in such a way can we combat and limit the spread of false identification information and SSN misuse. Similarly, all law enforcement should be provided the same SSN verification capabilities currently granted to employers.

We need legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. If we are to head off the many crimes identity theft breeds, we need legislation to restrict sale of SSNs by government agencies, to prohibit display of SSNs on government checks, drivers' licenses, vehicle registrations, and prohibit sale, purchase, or display of the SSN in the private sector.

I applaud the decision of the Treasury Department to remove SSNs from all Treasury checks, including Social Security and Supplemental Security Income checks, to protect the privacy of the SSN and reduce opportunities for identity theft. This good decision needs to be codified into law.

I describe other needed legislative changes in my written statement. With such legislation and the continuing dedication of the government agencies involved and of this Special Committee, I am confident that we can reverse the trend of identity theft against older Americans. Thank you very much.

Senator CRAIG. Thank you very much. We will visit at length about your suggestions about the use of the SSN and how it ought not be used. I think those are very valuable suggestions.

[The prepared statement of Mr. Huse follows:]

Statement for the Record -James G. Huse, Jr.

07/18/2002

Hearing on Identity Theft and America's Senior Citizens

Senate Special Committee on Aging

Good morning, Chairman Breaux, Ranking Member Craig, and members of the Senate Special Committee on Aging. I want to commend you for holding this important hearing today on identity theft and America's senior citizens.

Criminals do not steal the identities of the elderly so they can pretend to be old and wise. They do it because senior citizens are more likely than most of us to have significant assets--savings, investments, paid-up mortgages, good credit, and Federal entitlement checks. People over age 50 control at least 70 percent of the Nation's household net worth.

Some senior citizens are easier and safer to rob because they are less sure of themselves, more trusting, and less aware of simple precautions. They may be less likely to review their monthly financial statements. They may hesitate to take action if they *do* find something wrong because they are afraid a relative is responsible for robbing them, or because they are afraid they will make their families feel they can no longer be trusted to live independently. As the Federal Trade Commission (FTC) Identity Theft Data Clearinghouse has reported, incidents of identity theft targeting persons over the age of 60 increased from 1,821 victims in 2000 to 5,802 victims in 2001, a threefold increase. Anybody can steal candy from a baby, but criminals know our older Americans have money for the taking and they don't cry out loud.

Identity theft is an "enabling" crime, one that permits criminals to commit *other* crimes more effectively. Those crimes may range from passing bad checks and defrauding credit card companies to horrific acts of terrorism. In most cases, identity theft begins with the misuse of the Social Security number (SSN). No aspect of the Social Security Administration's (SSA) Office of the Inspector General's (OIG) mission of protecting Social Security programs from fraud, waste, and abuse is more important than our oversight of the use--and misuse--of the SSN.

There is an almost infinite variety to these cases.

- The New York Times reported recently that thieves are finding houses owned by elderly people, assuming the identity of the true owners and stripping equity out of the houses without their owners' knowledge or consent. In two such cases in Detroit, the Federal Bureau of Investigation (FBI) made its case and identified thieves through resources of the Identity Theft Task Force of Federal, State and local authorities. We serve on that task force with State and local police, various prosecutors, the FBI, Secret Service, and the Postal Inspection Service. The Privacy Rights Clearinghouse says the home sale racket is one of the more innovative types of identity theft officials are encountering.

- Our agents in San Diego were alerted when local law enforcement became suspicious as to the validity of an SSN presented by a man they were questioning. We found that the SSN belonged to a 70 year-old South Dakota woman. This man had been a fugitive felon for 17 years, with 4 prior felony convictions including prison escape. He had created, through the use of fraudulently obtained or counterfeited identification documents, 33 separate and distinct identities. Some were stolen, while others were entirely fictitious. He had used them not only to avoid capture, but to obtain employment as the chief of a fire department, the security chief for a county fair, and other positions of trust. He also committed bank fraud by obtaining credit cards and loans under his assumed identities while receiving Social Security benefits under three of his identities.

- Our Office of Investigations went after a man in Phoenix who had purposely engaged in telemarketing activity targeting individuals who were alone and elderly, and who hoped for something which would give them a better life. His practice generally involved an amount of money less than $500, which made the victim less likely to pursue legal action. He devised telemarketing schemes to defraud SSA beneficiaries, as well as other fraudulent lottery schemes through the mail, for a loss to the victims of approximately $1.3 million. He would send correspondence to these seniors bearing the words "Social Security Administration" and the official SSA seal, advising them they had been approved to receive an additional SSA benefit check, but they would have to pay a "processing fee" ranging from $9 to $99. In some cases, he requested banking

information in order to process the fee, and after receiving that information, he withdrew money directly from their checking accounts.

From October 1994 to October 1998, this same man mailed letters and made phone calls using the names Rainbow International, Magic Numbers, and Future Concepts to tell seniors they were part of a group that could participate in pooled lottery winnings upon payment of a processing fee. When individuals mailed checks to one of several mailboxes he maintained at commercial mail receiving companies, he used their signatures and created fictitious authorization forms to gather information, and again withdrew money from their checking accounts.

After our investigation resulted in a 14-count indictment, the man pleaded guilty to mail fraud. The judge termed his activity "despicable," and sentenced him to 36 months incarceration, a special assessment fee of $100, a fine of $7,500, restitution to the 20 victims of approximately $6,736, and deportation. The special conditions of supervised released included that he not enter into any major financial purchases or obligations without the approval of probation, that he cooperate with the Internal Revenue Service to file tax returns, and that he not engage in telemarketing or the sale of discount merchandise unless in a retail establishment.

- A Virginia man used an SSN to steal an elderly man's identity so he could work under the stolen SSN while continuing to collect disability benefits he no longer deserved under his own number. While using the SSN, he also took out over $24,000 worth of loans and credit for goods and services purchases. The older man's credit was damaged, and his Social Security benefits were interfered with because of the earnings posted to his earnings record at SSA. We got the identity thiefand the courts made him repay SSA and the creditors. He was also incarcerated for 1 year, received 3 years of supervised released and was ordered to pay a $100special assessment. But he created a lot of needless hassles for the victim and the financial institutions.

These are not necessarily small operations with solitary victims.

- One investigation we conducted confirmed that over 25,000 people, residents of nearly every State, had been duped by anonymous hoax

flyers. Such flyers, which were widely distributed to the elderly, falsely promised recipients they would receive money from the government if they mailed information to a post office box listed on the flyer. One flyer promised $5,000 pursuant to a fictional "Slave Reparations Act." Another promised an unwarranted lump sum payment or an increase in SSA benefits. "Notch Babies" (persons born between 1911 and 1926) were urged to become part of a "National Victims' Register" by sending in a variety of personal information. These flyers required the recipient to provide sensitive personal information such as name, address, telephone number, SSN, and date of birth. Many elderly Americans were so thoroughly confused by the flyers, that they sent copies of identity documents, including Social Security cards, driver's licenses, birth certificates, and military papers to the address on the flyers. By falsely promising additional Social Security payments, the anonymous mailings tricked them into parting with a wealth of personal information. Congress has helped us alert seniors to such frauds.

- We also brought a series of enforcement actions in Texas, in which several companies were ordered to stop sending deceptive Social Security-related advertisements, primarily to senior citizens. Acc-U-Lead, Inc., United States Senior Services, Inc., Mass Mail Media, Inc. and Lead Marketing Alliance, all Texas companies, were ordered to cease such mailings. The founders were also directed to pay penalties of $200,000 to SSA. These payments were part of a settlement in a case brought by our office and the U.S. Attorney's Office regarding government look-a-like documents that appeared to be from SSA. The government's case alleged that these companies sent misleading solicitations that used terms such as "Social Security Supplement Policy" or "2001 Benefit Update," when in reality the solicitations were meant to entice senior citizens to provide sensitive personal information. The defendant companies would then sell this data to private insurance companies and/or agents for up to $16 for each senior's reply. The data purchasers would then contact the seniors and pitch various products such as burial insurance and other related policies. As a result of such deceptive practices, the companies generated substantial revenues over several years from the sale of this sensitive personal information, unwittingly provided by seniors.

These stories illustrate that identity theft is a mushrooming reality. Though it is not a new phenomenon, today's computer technology makes it a great deal easier than it used to be. Amassing somebody's personal details is facilitated by

the plethora of databases available today. We each leave markers in our daily commerce -- in credit card charges, loan applications, medical questionnaires, and so on. They are recorded, aggregated, and resold by information brokers without our knowledge and consent, as if they owned our good names. This process of assembly and dissemination is overly facile and extremely fast because of our modern information media. There are seldom sufficient checks and balances to these activities, and too many have access to these details about all of us.

Typically, the victims of such scams are elderly individuals who have a trusting relationship with SSA. Such advertisements cleverly play to their desire for more Social Security-related information or additional Social Security benefits. Many victims never even realize that they have been tricked into parting with their personal information--they simply assume that SSA never responded to their request for information.

Senior citizens need to be alerted continuously to the dangers of giving away such information. They must be told about toll-free numbers, such as our Fraud Hotline (1-800-269-0271), and Internet sites, such as our oig.hotline@ssa.gov, where they can check on suspicious government mailings. They must be asked to *be* suspicious of purported government mailings that offer free money in exchange for personal information.

The victims are often scarred emotionally. They feel violated and helpless -- and very angry. I've talked to many who were psychologically overwhelmed, because they could not stop what was happening to them. I've talked with elderly people who were terrified of losing their life savings and their homes. Their lives are seriously disrupted because someone else's crooked credit history is recorded on their credit report. In 1999, a Privacy Rights Clearinghouse survey found the average amount of time spent by victims to regain their financial integrity was 175 hours, over a period of 2 years, at an average cost of over $800.

Congress enacted *The Identity Theft and Assumption Deterrence Act* in 1998 and *The Internet False Identification Prevention Act* in 2000. The former was the first legislative response to the growing epidemic of identity thefts and imposed criminal sanctions for those who create a false identity or misappropriate someone else's. The latter closed a loophole left by the first, enabling my office and other law enforcement organizations to pursue those who previously could sell counterfeit Social Security cards legally by maintaining the fiction that such cards were "novelties" rather than counterfeit documents. Both pieces of

legislation are helpful, but both treat the disease of identity theft in its later stages, rather than at the onset.

The ability to *prevent* identity theft is even more essential. Previously, I've said that the time has come to put the SSN back into its box. While we cannot return the SSN to its original limited function because of the complexity of how the SSN is used today, we must take steps to limit its use and to limit the *expansion* of its use. First and foremost, the time has come to make the difficult determinations as to those uses that are appropriate and necessary, and those that are merely convenient. The SSN has become a *de facto* national identifier and its daily use has, in many instances, become a luxury we can no longer afford. Similarly, the availability of SSNs on public documents and over the Internet must come to a stop.

Congress should consider requiring the cross verification of SSNs through both governmental and private sector systems of records. Only in such a way can we combat and limit the spread of false of identification and SSN misuse. Similarly all law enforcement should be provided the same SSN verification capabilities currently granted to employers.

We need legislation that regulates the use of the SSN and provides enforcement tools to punish its misuse. If we are to head off the many crimes identity theft breeds--the fraud against public and private institutions, the ruin of people's security, possibly even the disguising of terrorists as ordinary people--we need legislation with provisions such as:

- Restrictions on the private and governmental use of SSNs. This should include restrictions on the sale of SSNs by governmental agencies, prohibition of the display of SSNs on government checks and driver's licenses or motor vehicle registrations, and some prohibitions of the sale, purchase, or display of the SSN in the private sector.

- Prohibitions of inmate access to SSNs.

- Refusal to do business without receipt of an SSN could be considered an unfair or deceptive act or practice.

- Confidential treatment of credit header information.

In this vein, I applaud the decision announced last week by the Department of the Treasury to remove the SSN from all Treasury checks, including Social Security and Supplemental Security Income checks, as part of Treasury's efforts to protect the privacy of the customer's SSN and help reduce the opportunity for identity theft. This good decision needs to be codified into law.

Parallel legislative changes are needed that do not bear directly on identity theft, but which would also add protections for older Americans and others. They would include:

- Amending the Social Security Act provisions to direct, with certain limitations, the Commissioner of Social Security to fully reimburse Social Security beneficiaries for any part of their benefit that was misused by a representative payee. There are currently about 5 million representative payees who are appointed to receive and apply the benefits of Social Security recipients who cannot manage their own affairs. The potential for harm to seniors is obvious. It would also make good sense to bar the appointment as representative payees of fugitive felons, attorneys who have received certain sanctions, and people who have been convicted of any offense under Federal or State law resulting in imprisonment for more than one year, unless the Commissioner deems their appointment to be appropriate.

- Dishonest representative payees seem to think they have permission to appropriate the identities they are supposed to represent. Recently we worked with the Department of Veterans Affairs (VA) OIG to put away a Kansas man who was representative payee for several older recipients of VA and SSA benefits. He had stolen their benefits to keep his wife satisfied and to pay for his drinking habit, and had sold at least three recipients' farms for more than $70,000 each.

- Strengthening existing provisions of the Social Security Act that prohibit the misuse of symbols, emblems, or names in reference to Social Security or Medicare, to help combat the frauds that lead trusting seniors to send their identity information to criminals who pose as Government agencies.

With such legislation, and the continuing dedication of the Government agencies involved, and of this Special Committee, I am confident that we can reverse the trend of identity theft against older Americans. SSA, my office, the

Congress, and the American people must act together to accord both the SSN and our senior citizens the protections against identity theft that both deserve.

Thank you, and I'd be happy to answer any questions.

Senator CRAIG. Now, let us turn to Howard Beales, Director, Bureau of Consumer Protection, the Federal Trade Commission here in Washington. Howard, welcome before the committee.

STATEMENT OF HOWARD BEALES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, DC

Mr. BEALES. Thank you, Senator Craig and Senator Collins. Thank you for the opportunity to be here today to speak to you today about the crime of identity theft, which is a complex and pernicious problem in today's society. It is a crime that cuts across all lines of our population. Last year, we received complaints from just over 86,000 victims, including the elderly.

In 1998, Congress recognized the seriousness of this problem by making identity theft a Federal crime. Although the FTC does not have criminal law enforcement authority, we play a central role in assisting law enforcement and in helping victims recover. Under authority given to us by Congress, we have implemented a dedicated program to respond to ID theft. This program has three central features: Assisting consumers through complaint handling and steps to ease recovery; supporting law enforcement by making these victims' complaints available to State and Federal agencies for their use in investigations; and educating consumers on how to prevent and how to recover from identity theft.

The centerpiece of our program is our toll free number for identity theft victims, 877–ID–THEFT. Callers are connected with trained counselors who take their complaints and walk them through the steps to repair the damage done by identity thieves. Consumers can also enter their complaints via an online complaint form. From both the web complaint form and from telephone contact, we gather information about the incident, what happened to the victim, what is known about the suspect, and any special problems the victim may be encountering.

These data, in turn, are used to support and to enable more effective law enforcement investigations. Using our secure web-based Consumer Sentinel network system, law enforcement officers, from local sheriffs to the U.S. Secret Service, can access the more than 189,000 complaints that are now in our database. They can use that information to track down witnesses, to identify trends, or to look at information relating to their region or their ongoing cases.

Using the Secret Service's clustering software and supported by research from other law enforcement databases, we also develop preliminary investigative reports, which we send out to the U.S. Secret Service's Financial Crimes Task Forces and to other law enforcement agencies throughout the country to both assist and encourage investigations and prosecutions.

To further support the prosecution of identity theft, we are now training local and State law enforcement officers throughout the country. Sponsored jointly with the Justice Department and the Secret Service, the training focuses on how to investigate identity theft and how to coordinate with the Federal resources that are available to State and local authorities.

Coordination at all levels is particularly important in fighting identity theft because it is a crime that does not respect geographic

boundaries. We have already trained about 450 officers from over 110 agencies during the past 4 months and more sessions are planned. We continue to develop more and better ways to get the complaint data and other resources into the hands of those who could best pursue investigations and prosecutions.

Finally, consumer education plays a key role in our identity theft program. While no one can completely protect themselves from identity theft, there are steps we can all take to minimize our vulnerability.

For example, we advise consumers to be mindful of exposing their personal information, in particular, destroying financial documents before throwing them out and not leaving behind credit card receipts in stores and restaurants. We include such guidance in our booklet, "ID Theft: When Bad Things Happen to Your Good Name," as well as step-by-step advice for victims on how to repair the damage caused by identity theft. To date, we have distributed more than 1.5 million copies, both in hard copy and via our website. Other agencies, including the Social Security Administration, the SEC, and the FDIC, also print and distribute the booklet, as do many private sector organizations. We recently released a version in Spanish.

Despite these efforts, the risk of identity theft remains real for all Americans, including those aged 60 and over. To determine whether the elderly are particular targets for identity thieves, we examined the complaints in our database. That analysis shows that older Americans experience more or less the same types of identity theft at roughly similar rates to others.

In 2001, our clearinghouse received 5,800 complaints from victims who were 60 and over. That constitutes 10 percent of the complaints where the victims provided their age. In contrast, this age group is 16 percent of the U.S. population. Without doing a survey of the population, we are unable to say whether they are simply less likely to be victims of identity theft or if they are just less likely to report it. It is very difficult for us to separate those two possibilities in our data.

Americans over 60 experience the same types of identity theft and at more or less the same rates as those under 60. While there are some variations, for example, senior identity theft victims report slightly more credit card fraud than other age groups, they also report less employment-related identity theft, but there is nothing that signals that older Americans in general are more or less vulnerable in any particular way from other members of the population.

We do take special care in our consumer education and outreach efforts to reach older consumers. We work closely with the SSA, which distributes our booklet, and we have also worked closely with AARP, which has run many stories in its publications, referring members to our website and toll-free numbers and using our statistics to help explain identity theft.

In conclusion, despite the efforts of Congress and Federal and State and local law enforcement agencies, identity thieves remain among the most insidious and opportunistic of criminals, preying without prejudice on all segments of our population. The financial and emotional toll paid by the victim, however, is likely to be par-

ticularly egregious when the victims are elderly, who have worked a lifetime to establish good credit, only to have it ruined by these insidious thieves. Their acts are heinous and the FTC will continue to place a high priority in assisting law enforcement agencies in their efforts to identify and prosecute these criminals, as well as advising older Americans on steps they can do to reduce the risk of this crime.

Thank you, and I look forward to your questions.

Senator CRAIG. Howard, thank you very much.

[The prepared statement of Mr. Beales follows:]

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION ON

IDENTITY THEFT: THE IMPACT ON SENIORS

Before the

SENATE SPECIAL COMMITTEE ON AGING

Washington, D.C.

July 18, 2002

I. INTRODUCTION

Mr. Chairman, and members of the Committee, I am Howard Beales, Director of the Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to present the Commission's views on the impact of identity theft on the nation's seniors and describe to you the Commission's efforts to help victims, alert industry and equip law enforcement to deal with this harrowing crime.

The Federal Trade Commission has a broad mandate to protect consumers. In fact, the last time I testified on behalf of the Commission before this Committee, I addressed the issue of health fraud and the elderly.[2] Like the issue of health fraud, controlling identity theft is an important issue of concern to all consumers. Our activities in the area of identity theft differ in certain respects from our traditional enforcement role under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a), which prohibits unfair and deceptive acts and practices. Our primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act").[3] The Act directed the Federal Trade Commission to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education.

---

[1]The views expressed in this statement represent the views of the Commission. My oral presentation and responses to questions are my own and do not necessarily represent the views of the Commission or any Commissioner.

[2]"*Health Fraud and the Elderly: A Continuing Epidemic*" 107th Cong. (2001) (Prepared Statement of the Federal Trade Commission) (presented by Bureau Director J. Howard Beales).

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

In responding to the Identity Theft Act's directives, we have learned much about the crime, its victims, and its perpetrators. As discussed below, most victims who contact us report their age, and we have analyzed our data to assess how identity theft impacts senior Americans. Our analysis indicates that although consumers over 60 represent 16% of the population, they represent only 10% of our ID theft complainants. Overall, their experiences appear quite similar to the experiences of other consumers. Nonetheless, persons over 60 who provide their complaints to us report the most common form of identity theft -- credit card fraud -- at a slightly higher level than the population under 60 years of age. As in all aspects of our consumer protection mission, however, such as health care and telemarketing fraud, we remain keenly vigilant in protecting senior Americans through consumer education and support of law enforcement.

II. THE FEDERAL TRADE COMMISSION'S ROLE IN COMBATING IDENTITY THEFT

A. The Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft Act addressed identity theft in two significant ways. First, the Act strengthened the criminal laws governing identity theft.[4] Second, the Act specifically focused on consumers as victims.[5] On this second feature, the Act provided for a centralized complaint and

---

[4]18 U.S.C. § 1028(a)(7). The statute broadened "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual," including, among other things, name, address, social security number, driver's license number, biometric data, access devices (*i.e.*, credit cards), electronic identification number or routing code and telecommunication identifying information.

[5]Because individual consumers' financial liability is often limited, prior to the passage of the Act, financial institutions, rather than individuals, tended to be viewed as the primary victims of identity theft. Setting up an assistance process for consumer victims is consistent with one of the Act's stated goals: to recognize the individual victims of identity theft. *See* S. Rep. No. 105-

(continued...)

consumer education service for victims of identity theft. The Act specifically directed that the Commission establish procedures to: (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting agencies and law enforcement agencies.[6]

B. The FTC's Response to Identity Theft

In enacting the Identity Theft Act, Congress recognized that coordinated efforts are essential to best serve the needs of identity theft victims because these fraud victims often need assistance both from government agencies at the national and state or local level and from private businesses. Accordingly, the FTC's role under the Act is primarily one of facilitating information sharing among public and private entities.[7] In order to fulfill the purposes of the Act, the Commission has implemented a plan that centers on three principal components: (1) a toll-free telephone hotline, (2) the Identity Theft Data Clearinghouse, and (3) consumer education.

---

[5](...continued)
274, at 4 (1998).

[6]Pub. L. No. 105-318, § 5, 112 Stat. 3010 (1998).

[7]Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. J.K. Publications, Inc., et al,* 99 F. Supp. 2d 1176 (C.D. Cal. Apr. 10, 2000)(granting summary judgment for the FTC in case alleging that defendants obtained consumers' credit card numbers without their knowledge and billed consumers' accounts for unordered or fictitious Internet services), later proceedings at *FTC v. J.K. Publications, Inc., et al,* 99 Civ 00044 (C.D. Cal. Aug. 30, 2000)(final order awarding $37.5 million in redress); *FTC v. Rapp,* No. 99-WM-783 (D. Colo. filed Apr. 21, 1999) (alleging that defendants obtained private financial information under false pretenses)(Stipulated Consent Agreement and Final Order entered June 23, 2000).

(1) *Toll-free telephone hotline.* The Commission has established a toll-free telephone number, 1-877-ID THEFT (438-4338), that consumers can call to report identity theft. The identity theft hotline has been in operation since November 1, 1999. In 2001, we added more than 117,000 consumer reports to the Clearinghouse, up from slightly more than 44,000 in 2000. We do not attribute this dramatic growth in calls to a commensurate growth in the prevalence of identity theft. Rather, we see this increase as in part an indication of our successful outreach in informing the public of our program and the availability of assistance. Callers to the hotline receive telephone counseling from specially trained personnel to help them resolve credit-related problems that may have resulted from the misuse of their identities. In addition, the hotline counselors enter information from consumers' complaints into the Identity Theft Data Clearinghouse (the "Clearinghouse"), a centralized database used to aid law enforcement.

The counselors provide tailored information about preventing additional harm to consumers' finances and credit histories, including how to contact each of the three national consumer reporting agencies to obtain copies of their credit reports and request that a fraud alert be placed on their credit reports.[8] The counselors also advise consumers to review carefully the information on the reports to detect any additional evidence of identity theft. Consumers are informed of their rights under the Fair Credit Reporting Act and are given the procedures for correcting misinformation on their credit reports.[9] Consumers are also advised to contact each of the creditors or service providers where the identity thief has established or accessed an account to

---

[8] These fraud alerts indicate that the consumer is to be contacted when new credit is requested in that consumer's name.

[9] 15 U.S.C. § 1681 *et seq.*

request that the account be closed. The counselors also inform consumers of their rights under the Fair Credit Billing Act[10] and the Truth in Lending Act,[11] which, among other things, limit their liability for unauthorized charges in most instances. Consumers who have been contacted by a debt collector concerning debts incurred by the identity thief are advised of their rights under the Fair Debt Collection Practices Act, which prescribes debt collectors' practices.[12]

The telephone counselors also advise consumers to notify their local police departments, both because local law enforcement may be in the best position to catch and prosecute identity thieves, and because a police report often helps consumers demonstrate to would-be creditors and debt collectors that they are genuine victims of identity theft. Almost all of the states have enacted their own identity theft laws, and counselors, in appropriate circumstances, will refer consumers to other state and local authorities.

Lastly, where investigation and resolution of the identity theft falls under the jurisdiction of another regulatory agency that has a program in place to assist consumers, callers are referred to those agencies. For example, consumers who complain that someone has been using their Social Security number for employment are advised to report this to the Social Security Administration's fraud hotline and to request a copy of their Social Security Statement to verify the accuracy of the earnings reported to their Social Security number.

---

[10] 15 U.S.C. § 1666. The Fair Credit Billing Act generally applies to "open end" credit accounts, such as credit cards, revolving charge accounts, and overdraft checking accounts. It does not cover installment contracts, such as loans or extensions of credit that are repaid on a fixed schedule.

[11] 15 U.S.C. § 1601 *et seq.*

[12] 15 U.S.C. § 1692 *et seq.*

(2) *Identity Theft Data Clearinghouse*: The Identity Theft Act directed the FTC to log the complaints from victims of identity theft and refer those complaints to appropriate entities such as appropriate law enforcement agencies. Before launching our complaint system, the Commission took a number of steps to ensure that it would meet the needs of criminal law enforcement. For example, in April 1999, representatives from ten federal law enforcement agencies, five banking regulatory agencies, the U.S. Sentencing Commission, the National Association of Attorneys General and the New York State Attorney General's Office met at the FTC to share their thoughts on what the FTC's complaint database and comprehensive consumer education booklet should contain. The roundtable participants also established a working group that provided feedback throughout the construction of the database. The FTC opened the consumer hotline and began adding complaints to the resulting Clearinghouse in November 1999. Law enforcement organizations nationwide who were members of our Consumer Sentinel Network (the FTC's universal fraud complaint database) gained access to the Clearinghouse via our secure Web site in July of 2000.

To ensure that the database operates as a national clearinghouse for complaints, the FTC has solicited complaints from other sources. For example, in November 2000, the International Association of Chiefs of Police (IACP) unanimously passed a resolution in support of curbing identity theft which, among other things, calls upon local police to refer identity theft victims to the FTC's hotline so that their complaints will be available to law enforcement officers nationwide through the Clearinghouse. In February 2001, the Social Security Administration Office of Inspector General (SSA-OIG) began providing the FTC complaints from its fraud hotline,

significantly enriching our database. As a result of these efforts, the Clearinghouse has become a key element in identity theft investigations.

The Clearinghouse provides a much fuller picture of the nature, prevalence, and trends of identity theft than was previously available.[13] As the number of complaints entered into the Clearinghouse grows, it becomes a richer source of data for law enforcement, both in terms of developing and enhancing cases, and in providing information about the overall patterns and trends in identity theft.

Data from the Clearinghouse also assist law enforcement in other important ways. FTC data analysts aggregate the data to develop statistics about the nature and frequency of identity theft. Law enforcement and other policy makers at all levels of government use these reports to better understand the challenges identity theft presents. For instance, we publish charts showing the prevalence of identity theft by states and by cities. The data also demonstrate general trends. The first twelve months of data revealed that over thirty-five percent of victims who called us reported that they had not been able to file police reports. Following the November 2000 IACP resolution that called upon local police to write reports for all incidents of identity theft, the number of victims who were unable to file a report fell by almost half to eighteen percent.

Since the inception of the Clearinghouse, forty-eight separate federal agencies and three hundred thirty five different state and local agencies have signed up for access to the database. Among the agencies represented are over half the state Attorneys General as well as law

---

[13] Charts that summarize 2001 data from the Clearinghouse can be found at www.consumer.gov/idtheft and www.consumer.gov/sentinel.

enforcement from a number of major cities including Baltimore, Dallas, Los Angeles, Miami, San Francisco, and Philadelphia. We actively encourage even greater participation.

One of the goals of the Clearinghouse and the FTC's Identity Theft program is to provide support for identity theft prosecutions nationwide.[14] To further expand the use of the Clearinghouse among law enforcement, the FTC, in cooperation with the Department of Justice and the United States Secret Service, initiated a full day identity theft training seminar for state and local law enforcement officers. To date, we have held sessions in Washington, D.C., Des Moines, Chicago, and San Francisco. An August session is slated for Dallas. About 450 officers have attended these seminars, representing more than 110 different agencies.

FTC staff also help develop case leads. In the past year, the Commission launched an identity theft case referral program in coordination with the United States Secret Service, which assigned a special agent on a full-time basis to the Commission to assist with identity theft issues.[15] The identity theft team, assisted by the special agent, examines significant patterns of identity theft activity in the database and refines the data through the use of additional investigative resources, developing a preliminary investigative report. Then, the team refers the investigative report to one of the Financial Crimes Task Forces located throughout the country for further investigation and potential prosecution.

---

[14]The Commission recently testified in support of S. 2541, the Identity Theft Penalty Enhancement Act of 2002, which would increase penalties and streamline proof requirements for prosecution of many of the most harmful forms of identity theft. See Testimony of Bureau Director J. Howard Beales, Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information (July 11, 2002).

[15]The referral program complements the regular use of the database by all law enforcers from their desk top computers.

(3) *Consumer education*. The FTC has taken the lead in coordinating with other government agencies and organizations the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime.[16] The FTC's extensive, multi-media campaign includes print materials, media mailings and interviews, as well as the Identity Theft website, located at www.consumer.gov/idtheft. This collaborative consumer education effort is ongoing, and the Commission will continue such outreach with many of the private sector financial institutions that have an interest in preventing and remedying identity theft.

Our consumer education message has reached older Americans. Most prominently, AARP's Identity theft web page, www.aarp.org/confacts/money/identity, links directly to consumer.gov/idtheft. In addition, numerous issues of *My Generation* and the *AARP Bulletin* have included articles on identity theft, and have included references to the FTC's consumer education and assistance program.

The FTC's comprehensive consumer education booklet, *Identity Theft: When Bad Things Happen to Your Good Name*, has been a tremendous success. The 22-page booklet covers a wide range of topics, including how identity theft occurs, how consumers can protect their personal information and minimize their risk, what steps to take immediately upon finding out they are a victim, and how to correct credit-related and other problems that may result from identity theft. It

---

[16]Among the organizations the FTC brought into this effort are the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of Thrift Supervision, the Department of Justice, the U.S. Secret Service, the Federal Bureau of Investigation, the Postal Inspection Service, the Internal Revenue Service, the Social Security Administration, the Federal Communications Commission, the Securities and Exchange Commission, the U.S. Trustees, and the National Association of Attorneys General.

also describes federal and state resources that are available to consumers who have particular problems as a result of identity theft. The FTC has distributed more than 1.3 million copies of the booklet since its release in February 2000. We recently released a Spanish language version of the Identity Theft booklet (*Robo de Identidad: Algo malo puede pasarle a su buen nombre).*

Other governmental agencies have distributed *Identity Theft: When Bad Things Happen to Your Good Name* to their constituencies. The Social Security Administration has joined the SEC, the FCIC and other agencies in reprinting the booklet and distributing it to the public. The SSA's distribution of the book makes it more likely that it will reach older Americans.

The FTC also developed the identity theft website, www.consumer.gov/idtheft, which includes the booklet, descriptions of common identity theft scams, and links to testimony, reports, press releases, identity theft-related state laws, and other resources.[17] The affidavit, complaint form and Identity Theft booklet are offered in both English and Spanish. The site also has a link to a web-based complaint form, allowing consumers to send complaints directly to the Identity Theft Data Clearinghouse.

III. THE FTC'S RECENT COLLABORATIVE AND OUTREACH EFFORTS

Over the past year, the Commission has worked closely with other government agencies and private entities to encourage the investigation and prosecution of identity theft cases, and to help consumers resolve identity theft problems.

A. Private Industry

---

[17]www.consumer.gov is a multi-agency "one-stop" website for consumer information. The FTC hosts the server and provides all technical maintenance for the site. It contains a wide array of consumer information and currently has links to information from more than 170 federal agencies.

Identity theft victims spend significant time and effort restoring their good name and financial histories. That burden results, in part, from the need to complete a different fraud affidavit for each different creditor where the identity thief opened or used an account in their name.[18] To reduce that burden, the FTC worked to develop the ID Theft Affidavit. The affidavit was the culmination of an effort we coordinated with private industry and consumer advocates to create a standard form for victims to use in absolving identity theft debts with each of the creditors where identity thieves opened accounts. The affidavit is accepted by the three major credit reporting agencies and many creditors. From its release in August 2001 through June 2002, we have distributed more 160,000 print copies of the affidavit. There have also been more than 200,000 hits to the Web version. The affidavit is available in both English and Spanish.

The FTC is examining other ways to lessen the difficulties and burdens faced by identity theft victims. One approach under consideration is to develop a joint "fraud alert initiative" with the three major credit reporting agencies ("CRAs"). This initiative would allow the CRAs to share among themselves requests from identity theft victims that fraud alerts be placed on their consumer reports and copies of their reports be sent to them. This would eliminate the victim's need to contact each of the three major CRAs separately.

Additionally, the FTC is working with institutions that maintain consumers' information to identify ways to help keep that information safe from identity theft. In April, the FTC invited representatives from financial institutions, credit issuers, universities and retailers to a one day informal roundtable discussion of ways to prevent access to personal information such as

---

[18] *See ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.* 106th Cong. (2000) (statement of Mrs. Maureen Mitchell, Identity Theft Victim).

employee and customer records. Recent episodes of wholesale thefts of information highlight the importance of this effort among entities that hold sensitive information.[19]

B. Governmental Cooperation

The governmental response to identity theft is a model of interagency cooperation. The Attorney General's White Collar Crime Task Force's Subcommittee on Identity Theft, in which we participate, brings together representatives from agencies as diverse at state attorneys general, the State Department, the U.S. Postal Inspectors and the International Association of Chiefs of Police, among others. This group serves as a way to directly coordinate in such areas as legal developments, case generation, training, outreach and data-sharing.

Cooperation also takes the form of sharing personnel. The U.S. Secret Service has, for the second year, detailed a special agent to the FTC's identity theft program.[20] The agent has worked closely with FTC staff, helping to develop and lead the Identity Theft Investigations Training, outreach to law enforcement, and the development of the preliminary investigative reports.

IV. IDENTITY THEFT: THE IMPACT ON SENIORS

The data collected in our Identity Theft Clearinghouse provides important information on trends in identity theft. Consumers have absolute choice on how they share their data with us: none of the data fields is required. However, we do ask consumers to provide information on how

---

[19] Jacob Fries, *U.S. Says Ex-Prudential Worker Stole Colleagues' ID's and Sold them Online,* NY TIMES, March 2, 2002 at B2; John Schwartz, *13,000 Credit Reports Stolen by Hackers*, NY TIMES, May 17, 2002 at C5

[20] The Postal Inspection Service was the first agency to detail a law enforcement officer to work with the FTC's data sharing program. The Inspection Service detailed an inspector who, for over one year, managed our Consumer Sentinel system. These partnerships allow us to share expertise and also maintain open and ongoing communication.

the identity theft occurred, what they know about the suspect, and the response of creditors to their plight. We also request that consumers provide their age. While not all consumers disclose their age, we do receive age information from a sufficient number to allow us to focus on how older Americans experience identity theft.

A. General Trend Data for 2001

The FTC received more than 117,000 reports from both victims of identity theft and others concerned about identity theft in 2001. Thirteen percent of these records were contributed by the Social Security Administration's Office of the Inspector General, which operates a Consumer Fraud Hotline. Of the 117,000 reports, over 86,000 (75%) were complaints from actual victims of identity theft, and over 31,000 (25%) were inquiries about identity theft generally.

B. How Identity Theft Affects Older Americans

Having collected and analyzed two full years of data, we can begin to identify possible trends.[21] For example, in 2000, 70% of the 26,813 victims reporting to the FTC provided their age. In 2001, 88% of the 70,545 victims who contacted the FTC provided their age.[22] (Figure 1 sets out the age distribution of the 2001 victims.) Notwithstanding that increase in the number of those reporting their age, the breakdown across different age groups remained quite similar from 2000 to 2001. *See Figure 2.* Americans aged 60 and above represented about 10% of the

---

[21]Although our data do indicate that the actual numbers of complaints in all age groups more than doubled from 2000 to 2001, we cannot say that these numbers correspond necessarily to an equal increase in identity theft in the larger population. As noted above, the increase can also be attributed to a greater awareness of the FTC as a resource for ID theft victims.

[22] The SSA-OIG does not collect information about the victim's age. We therefore include only the 70,000 complaints received by the FTC in this statistical breakout.

complainants in both 2000 and 2001. This group represents about 16% of the population of the U.S. population overall.[23]

The 2001 Clearinghouse data show that there are some ways that identity theft varies for those over 60 years of age.[24] *See Figures 3-4.* While the data reveal differences between the age groups, they currently do not enable us to draw any conclusions explaining these differences.

- *Credit Card Fraud:* About 52% of the victims over age 60 in the Clearinghouse reported that either a new account was opened in their name, or someone took over an existing account, in comparison to approximately 45% of those under 60. This is the leading form of fraud for all victims.
- *Telecommunications or Utility Fraud:* About 15% of the victims over age 60 in the Clearinghouse report that the identity thief obtained unauthorized telecommunications or utility equipment or services in their name in comparison to approximately 24% of those under age 60. Frequently, this type of fraud involves the purchase of cellular phones and service.
- *Bank Fraud:* About 10% of all victims over age 60 reported fraud on their demand deposit (checking or savings) accounts in comparison to 14% of those under 60.
- *Fraudulent Loans:* Seven percent of all victims over age 60 reported that the identity thief obtained a loan in their name in comparison to about 8% of those under age 60.

---

[23] U.S. Census Bureau, Census 2000 - http://www.census.gov/prod/cen2000/dp1/2khus.pdf

[24] Because victims can report experiencing more than one form of identity theft, the percentages add up to more than 100%.

- *Employment Fraud:* About 2% of the victims over age 60 in the database reported that the identity thief used their personal information for employment purposes in comparison to approximately 8% of those under age 60.
- *Government Documents or Benefits Fraud:* About 3% of all victims over age 60 reported that the identity thief obtained government benefits or forged or obtained government documents in their name in comparison to about 7% of those under age 60.
- *Other Identity Theft:* About 9% of the victims over age 60 in the database reported various other types of identity theft in comparison to about 15% of those under age 60.
- *Attempted Identity Theft:* Almost 20% of victims over age 60 reported that someone had attempted to misuse their information in comparison to almost 11% of those victims under age 60.

Overall, this data show very similar experiences between ID theft victims over 60 and those under 60. Without a more intensive survey of identity theft victims, we can only surmise why, for example, those over 60 experience proportionately more credit card fraud and less fraud involving utilities and telecommunication. However, we do know that our response to identity theft must continue to focus on consumer education, support of law enforcement and cooperation with the private sector in identifying ways to protect consumers from this serious crime.

IV. CONCLUSION

Identity theft knows no barriers. Spanning the spectrum from young to old, rich to poor, identity theft has reached into every pocket of our population. Our response must be equally expansive. We will continue to identify ways to reach out through consumer education efforts, partnering with public and private agencies that reach different constituencies, and to support the prosecution of this crime. We will be particularly vigilant in looking for ways to reach American seniors with our consumer education message.

Figures and Trends on Identity Theft

provided to

U.S. Senate
Special Committee on Aging
107th Congress

by

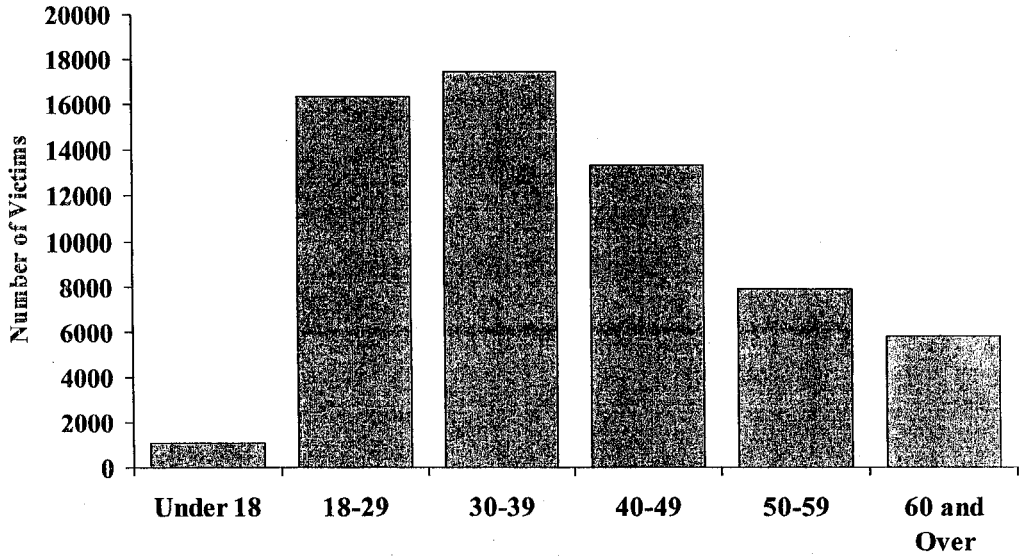
Federal Trade Commission
Washington, DC

Federal Trade Commission
Created July 1, 2002

IDENTITY THEFT Data Clearinghouse

Figure 1
Victim Age Distribution: Number of Victims[1]

January 1 – December 31, 2001



[1]This chart is based on reports from victims who contacted the FTC directly because external data contributors generally do not provide victim age information. During this time period, 88% (61,964) of victims reporting directly to the FTC (70,545) provided their age.

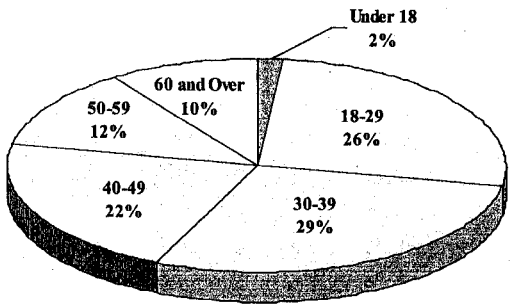
Federal Trade Commission
Created July 1, 2002

IDENTITY THEFT Data Clearinghouse

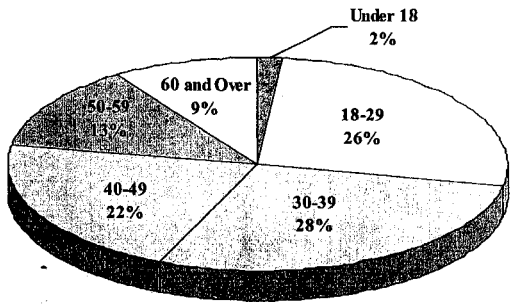
Figure 2
Victim Age Distribution: Percent of Victims[1]

January 1 – December 31, 2000 and
January 1 – December 31, 2001

January 1 – December 31, 2000



January 1 – December 31, 2001

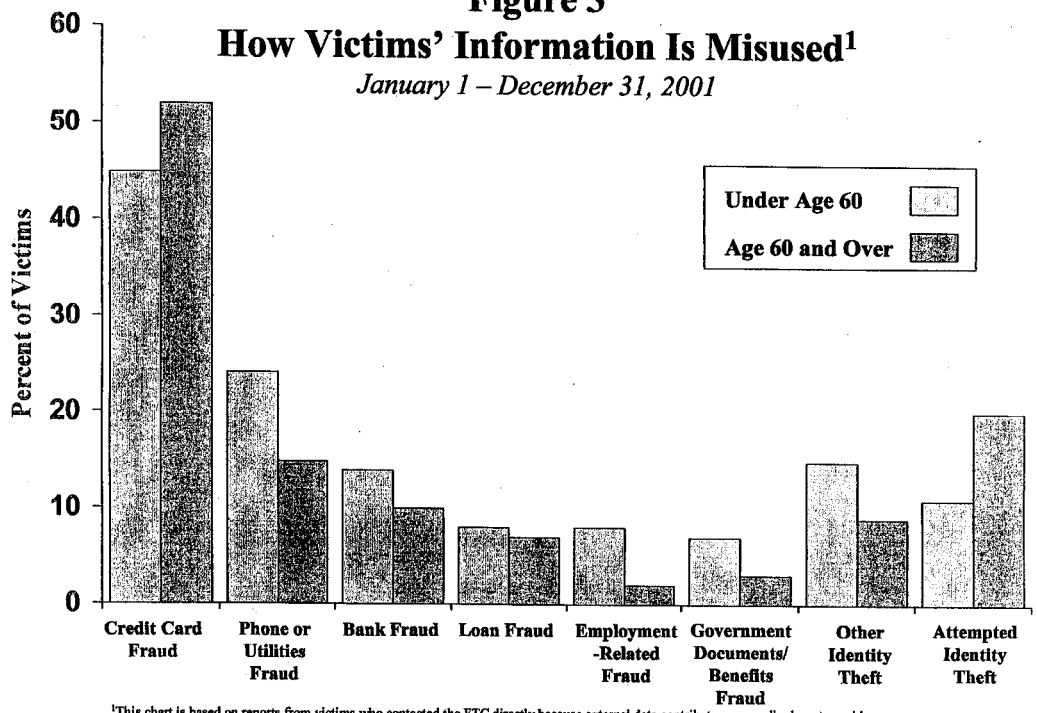


[1]This chart is based on reports from victims who contacted the FTC directly because external data contributors generally do not provide victim age information. From January 1 through December 31, 2000, 70% (18,879) of victims reporting directly to the FTC (26,813) provided their age. From January 1 though December 31, 2001, 88% (61,964) of victims reporting directly to the FTC (70,545) provided their age.

Federal Trade Commission
Created July 1, 2002

IDENTITY THEFT Data Clearinghouse

Figure 3
How Victims' Information Is Misused[1]
January 1 – December 31, 2001



[1]This chart is based on reports from victims who contacted the FTC directly because external data contributors generally do not provide victim age information. During this time period, 88% (61,964) of victims reporting directly to the FTC (70,545) provided their age. The columns sum to more than 100% because victims can report experiencing more than one type of identity theft.

Federal Trade Commission
Created July 1, 2002

Figure 4
How Victims' Information Is Misused[1]
January 1 – December 31, 2001

Theft Types	No. of Victims Under Age 60	Percent of Victims Under Age 60	No. of Victims Age 60 and Over	Percent of Victims Age 60 and Over
Credit Card Fraud	25,118	44.7%	2,995	51.6%
Phone or Utilities Fraud	13,305	23.7%	848	14.6%
Bank Fraud	7,858	14.0%	596	10.3%
Loan Fraud	4,602	8.2%	408	7.0%
Employment-Related Fraud	4,383	7.8%	95	1.6%
Goverment Documents/Benefits Fraud	3,773	6.7%	151	2.6%
Other Identity Theft	8,160	14.5%	537	9.3%
Attempted Identity Theft	6,119	10.9%	1,145	19.7%

[1]This chart is based on reports from victims who contacted the FTC directly because external data contributors generally do not provide victim age information. During this time period, 88% (61,964) of victims reporting directly to the FTC (70,545) provided their age: 56,162 victims under age 60 and 5,802 victims age 60 and over. The columns sum to more than the number of victims in an age category or more than 100% because victims can report experiencing more than one type of identity theft.

Federal Trade Commission
Created July 1, 2002

Senator CRAIG. Our last witness on this first panel is Doug Coombs, Deputy Special Agent in Charge, Financial Crimes Division, U.S. Secret Service. Doug, welcome to the committee.

STATEMENT OF DOUGLAS COOMBS, DEPUTY SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION, UNITED STATES SECRET SERVICE, WASHINGTON, DC

Mr. COOMBS. Thank you very much. Mr. Chairman, Senator Craig, Senator Collins, thank you for the opportunity to address this committee on the subject of identity theft and the Secret Service's efforts to combat the problem. I am particularly pleased to be here with my colleagues and partners in fighting identity theft from the Federal Trade Commission, Department of Justice, and the Social Security Administration.

With the passage of new Federal laws in 1982 and 1984, the Secret Service was provided jurisdiction for the investigation of the counterfeiting of identification documents and access device fraud. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crime.

The burgeoning use of the Internet and advanced technology, coupled with increased investment, has led to a great expansion within the financial sector. Although this provides benefits to the consumer through readily available credit and consumer-oriented financial services, it also creates a target-rich environment for today's sophisticated criminals, many of whom are organized and operate across international borders. Information collection has become a common byproduct of the newly emerging e-commerce and has led to an entirely new business sector being created which promotes the buying and selling of personal information.

As a result, the information consumers provide in credit card applications, loan applications, or with merchants they patronize are a valuable commodity in the new age of information trading. With the availability of this personal information, the crime of identity theft can be perpetrated with minimal effort on the part of even the relatively unsophisticated criminal.

Identity theft is not typically a stand-alone crime. It is almost always a component of one or more crimes, such as bank fraud, credit card or access device fraud, or the passing of counterfeit financial instruments. In many instances, an identity theft case encompasses multiples types of fraud and affects all Americans, regardless of age, gender, nationality, or race.

Obviously, the impact is magnified when it affects one of America's most valued assets, the elderly, as they represent a generation with a trusting nature that is easy to exploit. This group is particularly dependent on other caregivers for assistance, such as relatives, medical staff, service personnel, and oftentimes complete strangers. This dependency increases their vulnerability to certain schemes involving identity theft.

It has been our experience that criminal groups involved in financial fraud and identity theft are increasingly diverse and routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders to their criminal activities. By working

closely with other Federal, State, and local law enforcement, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise bridging jurisdictional boundaries. This partnership approach to law enforcement is exemplified by the 37 Financial and Electronic Crimes Task Forces the Secret Service has located throughout the country.

Another important component of the Secret Service's preventative investigative efforts has been to increase awareness of issues related to financial crime investigations in general and of identity theft specifically. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives. The Secret Service has assigned a Special Agent to the Federal Trade Commission on a full-time basis to support all aspects of their identity theft program.

The International Association of Chiefs of Police and the Secret Service have partnered to produce an "Identity Theft Roll Call" video geared toward local police officers throughout the nation. The purpose of this video is to emphasize the need for police to document a citizen's complaint of identity theft regardless of the location of the suspect. The video and its companion reference guide will provide offices with information that can assist victims with remediation efforts.

At the request of the Attorney General, the Secret Service joined an Interagency Identity Theft Subcommittee comprised of Federal, State, and local law enforcement agencies, regulatory agencies, and professional agencies. It meets regularly to discuss and coordinate investigative and prosecutive strategies, as well as consumer education programs.

All levels of law enforcement should be familiar with the resources available to combat identity theft and to assist victims in rectifying damage done to their credit. The Secret Service has already undertaken a number of initiatives aimed at increasing awareness and providing the training necessary to address these issues, but those of us in law enforcement and consumer protection communities must continue to reach out to an even larger audience and we must continue to approach these investigations with a coordinated effort. This is central to providing a consistent level of vigilance in addressing investigations that are multi-jurisdictional, while avoiding duplication of effort.

The Secret Service is prepared to assist this committee in protecting and assisting the nation's largest growing population segment with respect to prevention, identification, and prosecution of identity theft criminals.

That concludes my remarks. I will be glad to answer any questions that Senator Craig and Senator Collins might have. Thank you.

Senator CRAIG. Doug, panelists, thank you very much for your remarks.

[The prepared statement of Mr. Coombs follows:]

STATEMENT OF DOUGLAS COOMBS

Deputy Special Agent in Charge
United States Secret Service
Financial Crimes Division

Before the Special Committee on Aging

United States Senate

July 18, 2002

Mr. Chairman, I would like to thank you, as well as the distinguished Ranking Member, Senator Craig, for the opportunity to address the Committee on the issue of identity theft and the Secret Service's efforts to combat this problem. I am particularly pleased to be here with my colleagues and partners in fighting identity theft from the Federal Trade Commission, Department of Justice, and the Social Security Administration.

The Secret Service was originally established within the Department of the Treasury in 1865 to combat the counterfeiting of U.S. currency. Since that time, this agency has been tasked with the investigation of other Treasury related crimes, as well as the protection of our nation's leaders, visiting foreign dignitaries and events of national significance. With the passage of new federal laws in 1982 and 1984, the Secret Service was provided jurisdiction for the investigation of the counterfeiting of identification documents, as well as access device fraud. The explosive growth of these crimes has resulted in the evolution of the Secret Service into an agency that is recognized worldwide for its expertise in the investigation of all types of financial crimes.

The burgeoning use of the Internet and advanced technology coupled with increased investment had led to a great expansion of activity within the financial sector. Although this provides benefits to the consumer through readily available credit and consumer oriented financial services, it also creates a target rich environment for today's sophisticated criminals, many of who are organized and operate across international borders.

Information collection has become a common byproduct of the newly emerging e-commerce. Internet purchases, credit card sales, and other forms of electronic transactions are being captured, stored, and analyzed by entrepreneurs intent on increasing their market share. This has led to an entirely new business sector being created which promotes the buying and selling of personal information. Consumers routinely provide personal, financial and health information to companies engaged in business on the Internet. They may not realize that the information they provide in credit

card applications, loan applications, or with merchants they patronize are valuable commodities in this new age of information trading. With the advent of the Internet, companies have been created for the sole purpose of data mining, data warehousing, and brokering of this information. These companies collect a wealth of information about consumers, including information as confidential as their medical histories. Like all businesses, data collection companies are profit motivated, and as such, may be more concerned with generating potential customers rather than safeguarding their information to prevent its misuse by unscrupulous individuals. The private sector represents the first line of defense in identity theft and has a responsibility to safeguard the data that it has collected. The greater the protections that industry provides to the public, the fewer the opportunities for identity theft.

Based upon this wealth of available personal information, the crime of identity theft can be perpetrated with minimal effort on the part of even relatively unsophisticated criminals.

There is no area today that is more relevant or topical than that of identity theft. Simply stated, identity theft is the use of another person's identity to commit fraudulent activity.

Identity theft is not typically a "stand alone" crime. It is almost always a component of one or more crimes, such as bank fraud, credit card or access device fraud, or the passing of counterfeit financial instruments. In many instances, an identity theft case encompasses multiple types of fraud. According to statistics compiled by the FTC for the year 2001, 20% of the 86,168 victim complaints reported involved more than one type of identity theft. The major complaints, which include multiple types of reported fraud, were:

- **42%** of complaints involved credit card fraud – i.e. someone either opened up a credit card account in the victim's name or "took over" their existing credit card account;
- **20%** of complaints involved the activation of telephone, cellular, or other utility service in the victim's name;
- **13%** of complaints involved bank accounts that had been opened in their name, and/or fraudulent checks had been negotiated in the victim's name;
- **7%** of complaints involved consumer loans or mortgages that were obtained in the victim's name;
- **9%** of complaints involved employment-related fraud;
- **6%** of complaints involved government documents/benefits fraud; and
- **17%** of miscellaneous fraud, such as medical, bankruptcy, criminal, and securities fraud.

IMPACT

Identity theft, unlike many types of crime, affects all Americans, regardless of age, gender, nationality, or race. Victims include everyone from restaurant workers, telephone repair technicians, and police officers, to corporate and government executives, celebrities and high-ranking military officers. What victims do have in common is the difficult, time consuming, and potentially expensive task of repairing the damage that has been done to their credit, their savings, and their reputation. Obviously, the impact is magnified when it affects one of America's most valued assets, our senior citizens, as they represent a generation with a trusting nature that is easy to exploit. This group is particularly dependent on other caregivers for assistance, such as relatives, medical staff, service personnel, an oftentimes, complete strangers. This dependency increases their vulnerability to certain schemes involving identity theft.

LEGISLATION

In past years, victims of financial crimes such as bank fraud or credit card fraud were identified by statute as the person, business, or financial institution that incurred a financial loss. All too often the individuals whose credit was ruined through identity theft were not even recognized as victims. This is no longer the case. The Identity Theft and Assumption Deterrence Act, passed by Congress in 1998, represented a comprehensive effort to re-write the federal criminal code to address identity theft. This new law amended Section 1028 of title 18 of the United States Code to provide greater protections for victims of identity theft. These protections included:

- expanding the definition of victim to include not just those persons, businesses or institutions that incurred monetary loss, but also those individuals whose credit was compromised as a result of financial crimes such as bank fraud or credit card fraud;

- The establishment of the Federal Trade Commission (FTC) as the central clearinghouse for victims to report incidents of identity theft. This centralization of all identity theft cases allows for the identification of systemic weaknesses and provides law enforcement with the ability to retrieve investigative data at one central location. It further allows the FTC to provide victims with the information and assistance they need in order to take the steps necessary to correct their credit records;

- Sentencing potential and asset forfeiture provisions were enhanced to help to reach prosecutorial thresholds and allow for the repatriation of funds to victims; and

- The elimination of a significant loophole in existing statutes. Previously, only the production or possession of false identity documents was unlawful. With advances in technology such as E-commerce and the Internet, criminals did not need actual, physical identity documents to assume an identity. This legislative change made it

illegal to steal another person's personal identification *information* with the intent to commit a violation, regardless of actual possession of identity *documents*.

We believe that the passage of this legislation was the catalyst needed to bring together both the federal and state government's resources in a focused and unified response to the identity theft problem. Today, law enforcement, regulatory and community assistance organizations have joined forces through a variety of working groups, task forces, and information sharing initiatives to assist victims of identity theft.

Amendments later made to the Identity Theft and Assumption Deterrence Act of 1998 provided a two level increase and a minimum offense level of 12 for offenses involving (1) the possession or use of equipment that is used to manufacture access devices; (2) the production of, or trafficking in, unauthorized and counterfeit access devices; or (3) affirmative identity theft. This legislation also defined affirmative identity theft as the "breeding" of means of identification, and enhanced penalties under certain circumstances, such as the possession of five or more means of identification that were unlawfully produced.

These amendments also provided a revised minimum loss rule for offenses involving counterfeit or unauthorized access devices. Specifically, this rule requires that a minimum loss amount of $500 per access device be used when calculating the loss involved in the offense, with the exception of the possession, not the use of, telecommunications access devices, in which case the minimum loss per unused device is $100.

Finally, these amendments encouraged an upward departure if the offense level does not accurately reflect the seriousness of the offense. Examples of cases in which a departure may be warranted include those in which (1) an identity theft cause substantial harm to the victim's reputation or credit record; (2) an individual is arrested, or is denied a job, because of a misidentification that resulted from an identity thief; or (3) a defendant essentially assumed the victim's identity.

Violations of the Act are investigated by federal law enforcement agencies, including the Secret Service, the U.S. Postal Inspection Service, the Social Security Administration (Office of the Inspector General), and the Federal Bureau of Investigation. Schemes to commit identity theft or fraud may also involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or Social Security fraud, as well as violations of state law. Because identity theft is often connected to criminal activity that comes under the jurisdiction of the Secret Service, we have taken an aggressive stance and continue to be a leading agency for the investigation and prosecution of such criminal activity.

Finally, we aware of the legislation, S. 2541, recently proposed by the Administration and introduced by Senators Feinstein, Kyl, Sessions and Grassley. There are some excellent ideas included in this legislation that we believe will be highly useful in all of our efforts to combat the crime of identity theft.

SECRET SERVICE INVESTIGATIONS

Although financial crimes are often referred to as "white collar" by some, this characterization can be misleading. The perpetrators of such crimes are increasingly diverse and today include organized criminal groups, street gangs and convicted felons. This can be attributed to many factors including:

- The probability of high financial gain versus low sentencing exposure;
- The increased availability of goods or services which can be obtained on credit; and
- The proliferation of computer technology in our society that provides easy access to the information needed to commit many financial crimes, as well as a means for committing them remotely.

The personal identifiers most often sought by criminals are those generally required to obtain goods and services on credit. These are primarily social security numbers, names, and dates of birth.

The methods of identity theft vary. It has been determined that many "low tech" identity thieves obtain personal identifiers by going through commercial and residential trash, a practice known as "dumpster diving". The theft of both incoming and outgoing mail from mailboxes is a practice used equally as often by individuals and organized groups, along with thefts of wallets and purses.

With the proliferation of computers and increased use of the Internet, many identity thieves have used information obtained from company databases and web sites. A case investigated by the Secret Services that illustrates this method involved an identity thief accessing a public web site to obtain the social security numbers of military officers. In some cases, the information obtained is in the public domain, and in others, it is proprietary, and is obtain by means of a computer intrusion.

The method that may be most difficult to prevent is theft by a collusive employee. The Secret Service has discovered that individuals or groups who wish to obtain personal identifiers or account information for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency.

In most of the cases our agency has investigated involving identity theft, criminals have used another individual's personal identifiers to apply for credit cards or consumer loans. Less commonly, they are used to establish bank accounts, leading to the laundering of stolen or counterfeit checks, or are used in a check-kiting scheme.

The majority of identity theft cases investigated by the Secret Service are initiated on the local law enforcement level. In most cases, the local police department is the first

responder to the victims once they become aware that their personal information is being used unlawfully. Credit card issuers as well as financial institutions will also contact a local Secret Service field office to report possible criminal activity.

At the present time, the Secret Service does not compile statistics related to the age of victims for any type of investigation. The FBI's Uniform Crime Report, the premier crime statistic resource, does capture victim statistics, but only for the crime of murder. It should be noted, however, that due to the FTC's designation as the clearinghouse for consumer complaints, their statistics are readily available and delineated by geography, age, and type of fraudulent activity.

A significant probability exists that older Americans will become an increasingly attractive target by criminal elements given the fact that 70% of our nation's wealth is controlled by those 50 years of age and older. Additionally, the common perception is that it is difficult for elderly victims to repair the effects of identity theft due to a lack of technical knowledge and uncertainty on how to protect themselves. Often, the level of diligence in monitoring personal finances decreases among the elderly or, after discovering the fraudulent activity, some are embarrassed and unsure of the steps necessary to report the compromise.

COORDINATION

The Secret Service continues to attack identity theft by aggressively pursuing our core violations, which include violations involving counterfeit checks, counterfeit and fraudulently obtained credit cards, other counterfeit instruments, and false identification. Many of these schemes would not be possible without compromising the personal financial information of an innocent victim.

Our own investigations have frequently involved the targeting of organized criminal groups that are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal information to further their financial crime activity.

It has been our experience that the criminal groups involved in these types of crimes routinely operate in a multi-jurisdictional environment. This has created problems for local law enforcement agencies that generally act as the first responders to their criminal activities. By working closely with other federal, state, and local law enforcement, as well as international police agencies, we are able to provide a comprehensive network of intelligence sharing, resource sharing, and technical expertise which bridges jurisdictional boundaries. This partnership approach to law enforcement is exemplified by our financial and electronic crime task forces located throughout the country. These task forces primarily target suspects and organized criminal enterprises engaged in financial and electronic criminal activity that falls within the investigative jurisdiction of the Secret Service. Members of these task forces, which include local and state law enforcement, private industry and academia, pool their resources and expertise in a collaborative effort to detect and prevent electronic crimes.

While our task forces do not focus exclusively on identity theft, we recognize that a stolen identity is often a central component of other electronic crimes. Consequently, our task forces devote considerable time and resources to the issue of identity theft, including the "pure" identity theft cases that meet prosecutive guidelines and are consistent with the task force's case prioritization strategy.

Another important component of the Secret Service's preventative and investigative efforts has been to increase awareness of issues related to financial crime investigations in general, and of identity theft specifically, both in the law enforcement community and the general public. The Secret Service has tried to educate consumers and provide training to law enforcement personnel through a variety of partnerships and initiatives.

For example, criminals increasingly employ technology as a means of communication, a tool for theft and extortion, and a repository for incriminating information. As a result, the investigation of all types of criminal activity, including identity theft, now routinely involves the seizure and analysis of electronic evidence. In response to this trend, the Secret Service developed, in conjunction with the International Association of Chiefs of Police (IACP), the "Best Practices for Seizing Electronic Evidence Manual", to assist law enforcement officers in recognizing, protecting, seizing and searching electronic devices in accordance with applicable statutes and policies.

As a follow-up to this guide, the Secret Service and the IACP developed "Forward Edge"; a computer based training application designed to allow officers to "virtually" seize different types of evidence, including electronic evidence, at various crime scenes.

Further, the Secret Service, in conjunction with the U.S. Postal Inspection Service and the Federal Reserve Bank System, produced an identity theft awareness video. The video, which explains how easily one can become a victim and what steps should be taken to minimize damage, has been made available to Secret Service offices for use in public education efforts.

In April of 2001, the Secret Service assisted the FTC in the design of an identity theft brochure, containing information to assist victims on how to restore their "good name", as well as how to prevent their information and identities from becoming compromised.

Finally, the International Association of Chiefs of Police (IACP and the Secret Service have partnered to produce an "Identity Theft Roll-Call Video" geared toward local police officers throughout the nation. The purpose of this video is to emphasize the need for police to document a citizen's complaint of identity theft, regardless of the location of the suspects. In addition, the video and its companion reference card will provide officers with information that can assist victims with remediation efforts.

The Secret Service is also actively involved with a number of government-sponsored initiatives. At the request of the Attorney General, the Secret Service joined an interagency identity theft subcommittee that was established by the Department of

Justice. This group, which is comprised of federal, state, and local law enforcement agencies, regulatory agencies, and professional agencies, meets regularly to discuss and coordinate investigative and prosecutive strategies as well as consumer education programs.

Last spring, the Secret Service's Financial Crimes Division assigned a full time special agent to the FTC to support all aspects of their program to encourage the use of the Identity Theft Data Clearinghouse as a law enforcement tool. The Identity Theft and Assumption Deterrence Act established the FTC as the central point of contact for identity theft victims to report all instances of identity theft. The FTC has done an excellent job of providing people with the information and assistance they need in order to take the steps necessary to correct their credit records, as well as undertaking a variety of "consumer awareness" initiatives regarding identity theft. To date, the Secret Service representative at the FTC has:

- Met with and made presentations to federal, state and local law enforcement about the FTC's Identity Theft Data Clearinghouse and it's victim assistance program;

- Worked closely with agents in the field to ensure that they have access to the Consumer Sentinel system and are comfortable using the Identity Theft Data Clearinghouse database;

- Used the Identity Theft Data Clearinghouse to identify possible case leads, and developed a protocol for selecting which victim complaints are most likely to be successful case leads for criminal law enforcement agencies;

- Developed points of contact at the local, state and federal levels of government to receive case lead referrals from the Identity Theft Data Clearinghouse database, and also identified routines and procedures to be followed when referring such cases;

- Served as both a presenter and an instructor at 11 law enforcement training conferences hosted by various law enforcement agencies or organizations, such as the International Association of Financial Crimes Investigators (IAFCI) and the U.S. Marshal's Investigators Conference; and

- Coordinated and sponsored Identity Theft Seminars which have been attended by approximately 1,400 state and local law enforcement personnel.

It is important to recognize that public education efforts can only go so far in combating the growth of identity theft. Because social security numbers, in conjunction with other personal identifiers, are used for such a wide variety of record keeping and credit related applications, even a consumer who takes appropriate precautions to safeguard such information is not immune from becoming a victim.

PRECAUTIONS AND REMEDIES

The Secret Service recommends that consumers take the following steps to protect themselves from credit card fraud and identity theft:

- Maintain a list of all credit card accounts that is not carried in a wallet or purse so that immediate notification can occur if any cards are lost or stolen;
- Avoid carrying any more credit cards in a wallet or purse than is actually needed;
- Cancel any accounts that are not in use;
- Be conscious of when billing statements should be received, and if they are not received during that window, contact the sender;
- Check credit card bills against receipts before paying them;
- Avoid using a date of birth, social security number, name or similar information as a password or PIN code, and change passwords at least once a year;
- Shred or burn pre-approved credit card applications, credit card receipts, bills and other financial information that you do not want to save;
- Order a credit report once a year from each of the three major credit bureaus to check for inaccuracies and fraudulent use of accounts; and
- Avoid providing any personal information over the telephone unless you initiated the call, and be aware that individuals and business contacted via the Internet may misrepresent themselves.

Should an individual become the victim of identity theft, the Secret Service recommends the following steps:

- Report the crime to the police immediately and get a copy of the police report;
- Immediately notify your credit card issuers and request replacement cards with new account numbers. Also request that the old account be processed as "account closed at consumers' request" for credit record purposes. Ask that a password be used before any inquiries or changes can be made on the new account. Follow up the telephone conversation with a letter summarizing your requests;
- Call the fraud units of the three credit reporting bureaus, and report the theft of your credit cards and/or numbers. Ask that your accounts be flagged, and add a victim's statement to your report that requests that they contact you to verify future credit applications. Order copies of your credit reports so you can review them to make sure no additional fraudulent accounts have been opened in your name;

- Notify the Social Security Administration's Office of Inspector General if your social security number has been used fraudulently;

- File a complaint with the Federal Trade Commission (FTC) by calling 1-877-ID-THEFT or writing to them at Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580. Their website can also be accessed at www.ftc.gov/ftc/complaint.htm; and

- Follow up with the credit bureaus every three months for at least a year and order new copies of your reports so that you can verify that corrections have been made, and to make sure that no new fraudulent accounts have been established.

CONCLUSION

For law enforcement to properly prevent and combat identity theft steps must be taken to ensure that local, state and federal agencies are addressing victim concerns in a consistent manner. All levels of law enforcement should be familiar with the resources available to combat identity theft and to assist victims in rectifying damage done to their credit. It is essential that law enforcement recognize that identity theft must be combated on all fronts, from the officer who receives a victim's complaint, to the detective or Special Agent investigating an organized identity theft ring.

The Secret Service has already undertaken a number of initiatives aimed at increasing awareness and providing the training necessary to address these issues, but those of us in the law enforcement and consumer protection communities need to continue to reach out to an even larger audience. We need to continue to approach these investigations with a coordinated effort – this is central to providing a consistent level of vigilance and addressing investigations that are multi-jurisdictional while avoiding duplication of effort.

As you know, Mr. Chairman, the President has proposed transferring our agency and all of its functions to the new Department of Homeland Security. The Secret Service strongly supports this proposal, and we are confident that our ability to build partnerships with state and local law enforcement, as well as the private sector, will allow us to continue our preventative and investigative efforts with respect to identity theft as a leading agency in the new department.

The Secret Service is prepared to assist this committee in protecting and assisting the nation's largest growing population segment, with respect to the prevention, identification and prosecution of identity theft criminals.

Mr. Chairman, that concludes my prepared remarks and I would be happy to answer any questions that you or other members of the committee may have.

Senator CRAIG. Let me start with a brief line of questioning, then I will turn to Senator Collins, and then I may have additional questions.

John, what is the best advice you might give seniors who would be looking at this record or listening in to protect themselves from what happened to you and Mrs. Stevens?

Colonel STEVENS. First of all, so many people want your Social Security number. Do not give it to them unless there is a legitimate need for it, because that is the beginning of all the identity theft and it was the beginning of ours. We suspect——

Senator CRAIG. So it was the Social Security number that was the entry to your resources?

Colonel STEVENS. We suspect that they came off of the DOD computers that have access to my wifes and my Social Security numbers, under the DEERS and ID program that they were able to get that information on us. But the thing is, just be aware, do not talk to door-to-door salesmen that just happen to be in the neighborhood. Never fall for any of the telemarketing schemes. Always opt out whenever you have the opportunity, and if you do not, complain anyway so that it just cuts down on a lot of the junk mail that you have to shred. Generally, be aware of what is happening.

The major thing that you have to do is just stop giving out information indiscriminately. Everybody wants to find out about you, but do not answer the questions.

Senator CRAIG. John, do you know if those who perpetrated the crime against you and Mrs. Stevens were ever apprehended and prosecuted?

Colonel STEVENS. They have not been, but we suspect we know who they are and I think it was a person that probably had access to the DOD computers.

Senator CRAIG. How long ago was this? When did this start?

Colonel STEVENS. It started—we found out about it in March 1997.

Senator CRAIG. Ninety-seven.

Colonel STEVENS. This was by a phone call from then-Nations Bank wanting me to make payments on a Jeep Cherokee that was bought in Texas, and I am living in Maryland. I do not have a Jeep Cherokee. We found out that there were a total of five cars that were bought in our name and total damages—they totaled it up to $113,000.

Senator CRAIG. Alice, what is the single greatest challenges for prosecutors in obtaining a conviction in identity theft cases?

Ms. FISHER. I think the biggest challenge for all of us, as John said, is prevention and education of ways to prevent. But from a prosecutorial perspective, I would say that prompt reporting and aggressive review of financial data and reporting to State police, local police, Federal authorities, so we can investigate the case immediately. It gives us a better chance to find the culprit and then prosecute them. Once we find who did it, the prosecution actually is fairly straightforward. But it is finding the criminals.

In one case, I think it was out of Texas, it was 20 years before it was reported by the woman who was the victim of an identity theft because she did not regularly use credit cards, and the person that had committed the crime had used her Social Security number

to get drivers' license in some States, filed bankruptcy in another State, and was arrested in yet another State, and it was 20 years before they found it.

So I would say the challenge is to encourage people to report any suspicious activity promptly to the authorities.

Senator CRAIG. In this effort, is State law a problem?

Ms. FISHER. Actually, in the last 3 years, the States have really gotten on board in this problem and 47 States have passed identity theft laws. So we are real pleased in the way that they are coming along. We also coordinate through the Attorney General's Subcommittee on Identity Theft with the National Association of Attorneys General and the National Association of District Attorneys and the International Association of Chiefs of Police and reach out to chiefs of police all over the nation.

I would say that one of the things we would hope that the State and locals would do better is to fill out police reports better, because not only does that get us on board for enforcement, but it also helps victims, such as John, to use that police report to secure and restore their identity.

Senator CRAIG. Thank you.

Mr. Huse, in today's world of trying to develop single-digit, or multiple-digit but single-number IDs, we all want a universal phone number that we can use anywhere in the world, and in the wireless world, that is becoming increasingly the case. I think we all want to consolidate numbers as much as we can because we find our mind full of all kinds of access numbers and code numbers and that type of thing. Is there any prohibition now against the use of the SSN?

Mr. HUSE. No. The SSN is pretty much the de facto national identifier, and I think, as a people, we need to accept the fact that it has become that. It pervades almost every aspect of our governmental, financial, and commercial lives. We are our number, and I think that probably as a people, we do not want a national identity card, but we have a great ambiguity about the fact that the number has become very convenient for us to do business in this very complex world we have today. So I think, to answer your question, we need to live with the reality of what the number is and what it does and now look at ways to make its integrity stronger. I think that is the key.

Senator CRAIG. You had suggested that might be done by requiring limits in its application, I guess that is a better way of saying it?

Mr. HUSE. I think we need to look at how the number is used and how it is displayed and how it is aggregated in different data banks and databases by people who use it for commercial purposes. We need to regulate that. We have to be sure that the data in these stores, whether they are independent research companies or financial institutions or credit bureaus, we have to be sure that the data there is accurate and that the people that run those are responsible for that data. I think that is an obligation of government.

I think that those records need to be matched, not only commercial and financial records, but also all government records at local, county, State, and Federal records so that their data is accurate.

In that process, the anomalies will fall out and those become key law enforcement leads. I do not know any other way to fix this.

I have been involved in this for 32 years. I was a Secret Service agent long before I became an Inspector General. This is a problem that has a solution, but it involves a little bit more action. A lot has been taken, and I think this is the last step to really make it protected.

Senator CRAIG. This committee, and we will work with you, visit with you about that at length to see where we might make better use of your ideas.

Mr. Beales, is there a way to acquire reports of identity theft from credit reporting agencies to supplement your current database?

Mr. BEALES. Well, what we do right now is the credit reporting agencies refer people to us and we refer people to them, so that when people call us, we certainly tell them to call the credit reporting agencies to make sure that they get a copy of their credit report and make any corrections to their credit reports and the credit reporting agencies, when they get a complaint, they urge the victims to call the FTC to get our consumer education materials and also to report the offense for law enforcement purposes.

They need somewhat different data than we do and we get information about the nature of the crime that is useful to us that they do not particularly need. So it is not clear that direct sharing would be the most efficient way to go about it, simply because of the different information needs. But we do think we have good cooperation in referring consumers so that we probably are picking up most of those complaints, but we cannot tell for sure.

Senator CRAIG. Let me move on to Mr. Coombs and then my other colleagues, and Senator Tom Carper has joined us, and then I will come back to you, Mr. Beales, with another question.

Mr. Coombs, is there a danger that funds stolen through identity theft can become sources for funding terrorist activities domestically, or is there any evidence that that has ever occurred?

Mr. COOMBS. Prior to my current assignment as Deputy Special Agent in Charge in the Financial Crimes Division, I spent numerous years supervising and running a Counterfeit Crimes Task Force in Orange County, CA, and then a fraud squad in Los Angeles, CA, which is among some circles considered the identity theft capital of the world.

It is my experience that, as Senator Collins pointed out in her opening remarks, that fraud identification, credit card fraud, and stolen identities certainly have evolved to where they are the tools of the criminal of the 21st century, if you will. It is my experience that financial crimes and identity theft, which is often a component of financial crimes, is committed by a spectrum of the criminal element, if you will, from the drug dealer who needs to support a habit to organized criminal groups that it is part of their overall criminal portfolio, to the unsophisticated criminal who utilizes dumpster-diving as a means to compromise information, to the sophisticated technically savvy, if you will, criminal who utilizes hacking and maybe a scheming device to compromise this information.

It is the vulnerability of the information that is susceptible and is prone to identity theft. Therefore, it certainly is possible and feasible that terrorists could compromise information for financial gain, or more importantly, to create that cloak of anonymity to commit other types of crimes.

Senator CRAIG. Thank you very much.

Before I turn to Senator Collins for questions, let me turn to Senator Carper to see if he has any opening statement. Tom.

Senator CARPER. I do not. I am glad to be here and I am glad you are here, as well. I really just came to hear Susan Collins' questions. [Laughter.]

Senator COLLINS. Right.

Senator CRAIG. Here we go. Senator Collins?

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

Colonel Stevens, it was fascinating to hear that you first found out that your identity had been stolen when you got a call from a bank demanding payments on a Jeep that you did not own, and then you found out that there were five other cars or vehicles that had been purchased in your name.

I would like you to tell us a little bit about what you did when you realized this had happened to you and how cooperative were credit card companies, banks, and credit bureaus in your quest to straighten it out, because from my experience as a financial regulator at the State level, I know a lot of times, consumers felt extremely frustrated in trying to straighten out instances of just misidentity, where two people have the same name, much less identity theft. Could you tell us whether this has been a difficult process or not?

Colonel STEVENS. It is very difficult. The first thing, I had to get my wife down off the ceiling, because when she got all this information, she exploded. Thank goodness, I am partially deaf anyway, so——[Laughter.]

After the phone calls—in other words, to clear the Jeep Cherokee, I faxed them a copy of my driver's license. They faxed me a copy of the application. The only thing correct on it was the Social Security number and a smattering of my first and last name. The birthdays were wrong and everything else was wrong. In fact, if they had checked the birthdays and the issue date of the Social Security number, they would have found the Social Security number was issued before they were born. You know, just a simple check.

But we requested copies of the credit reports. Then we started to treat it like a—well, since I was in research and development for so long, we treated it like a project, systematically, with notebooks tracing down these creditors, because the credit bureaus did not have the information to contact them. So we would have to make numerous phone calls. I would go on the Internet and try to trace down an address and phone number.

So we finally contacted a majority of them and we would send them a sworn affidavit attesting to the fact that we did not do it. In other words, we are proving the negative. We did not do it. We are not the ones you are looking for.

So based on that, they would take that information and clear the account, or so we thought. Anyway, it disappeared from the credit report. Then again, they would turn up a little while later, a couple

of months later, in a third party collection agency. We have had some that have recycled as many as five times now. My wife just got notice of another one that was cleared and recycled again. It just keeps going on.

Senator COLLINS. So it is still going on even as we speak, 5 years later?

Colonel STEVENS. I described it once before as this birthday candle you blow out and it keeps relighting itself. [Laughter.]

It just keeps coming back.

Senator COLLINS. Mr. Beales, we have heard Mr. Stevens talk about how extremely difficult it is for him to restore his good credit and clear his name and that has been my experience in talking with consumers in Maine, as well. Obviously, Mr. Stevens describes himself as a warrior. He is undaunted. He is just going to keep pursuing this. But for a lot of seniors who are considerably older than Mr. Stevens and perhaps more intimidated by the process, this is a real problem.

Does the FTC actually assist individual consumers in clearing their record and restoring their good credit or are you just a repository for information and education about this?

Mr. BEALES. We are definitely a repository for information. We assist individual consumers in providing them with information and the steps to take, but we do not have the resources to do it on their behalf or to go as their advocate in dealing with the process. We try to explain the process, talk them through the process of what they have to do so they know what is coming, but they have to do it themselves.

Senator COLLINS. Mr. Chairman, I think that is a problem for a lot of our seniors and I do want, as part of this hearing, to let people know that most States have a Bureau of Consumer Credit Protection or something along that line which may be willing to intervene more directly for consumers.

Inspector General Huse, I want to follow up on the issue of the Social Security number because Mr. Stevens' case shows that that is the gateway to this crime in so many instances. I agree with you that the Treasury has taken a very important step by no longer printing the Social Security number on Social Security checks, but could you give us other examples of either legislative or administrative actions that you think should be taken to better safeguard that Social Security number, because once you have that, once the thief has that, it is very easy for him to get the other information he needs.

Mr. HUSE. It is the breeder identification, the Social Security number, in every possible context, to include in terrorists' activities, the use of numbers, identifying numbers, fake Social Security numbers. In the case of the September 11 terrorists, I think the Director of the FBI has testified to that, that that has been a result of their investigative efforts.

This number is so pervasively used, I think the obligation now is to make sure that the numbers themselves have some accuracy, and we have so many systems of records at local, county, State, and the Federal level, on just the governmental side. All those records should be accurate as to who I am, who you are, and what

our Social Security number is because it has become our identification.

That can be done by the Congress requiring periodic matching of that data so that all of those systems of records are accurate. If you take care of that, that is one piece. The Congress could consider making that requirement binding on the financial and commercial sector for the legitimate reasons that the number has been expanded to be used in commerce. We will never be able to pull that back unless we replace it with something else. That is a requirement, I think—that due diligence should be part of their ability to use the number.

The Social Security Administration itself has taken tremendous steps in the last few years to improve the business process of issuing the number. Now we have to fix the process of keeping the number accurate and strong in terms of integrity through its use. I think those are places we can work and find some solutions.

Senator COLLINS. Mr. Chairman, thank you. I know my time has expired. I do want to just let Ms. Fisher know that I am expecting a report from the Justice Department pursuant to the law on Internet identity theft. It has been over a year and I hope it will be forthcoming soon, because it does ask for legislative recommendations in this area. Thank you.

Senator CRAIG. Thank you.

Tom, questions?

Senator CARPER. Thank you. Yes, indeed.

About 5 years ago, one of our nieces down in North Carolina had her identity stolen and what occurred after that has been something I would not want to visit on anybody. On the one hand, there are the financial concerns and worries, but it is just as Mr. Stevens knows, just a huge pain in the neck to put up with—a lot of stress, a lot of worry, and a lot of aggravation.

I want to follow up on the question that Senator Collins presented to Mr. Huse. One of the questions I ask of panels is what should we do? You began to answer that question, and I would just ask of others at the table to do so as well. What should we do as legislators to address this problem? What is our obligation?

Mr. Huse, you have already spoken a little bit. I do not want to pick on you too much.

Mr. HUSE. I will only add one thing and then stop. The piece I also strongly believe in is that we have to grant law enforcement—because this crime is so pervasive and it cuts across all levels of government—we have to grant law enforcement at the local, county, State, and Federal level, but particularly those local law enforcement officers, the right to verify Social Security numbers, just as we allow employers to do that now on the wage and earnings side, to see if the person has the right to work.

That tool is critical in the early investigative stages of an identity theft case like Colonel Stevens. If local law enforcement can establish those identities as they are working the crime, a lot more can be done as we do now. This crime, because of the Internet and our modern technology, works so quickly, we need to give all of the tools we can to law enforcement.

Senator CARPER. OK, thank you. Others?

Mr. BEALES. Senator, I think S. 2541 is a very good idea, toughening the penalties and streamlining the proof requirements for identity theft is a good way to address the problem. I think hearings like this help to reduce the problems because they bring them to people's attention. That encourages people to report problems to us sooner, and we have definitely seen that trend in our database over the last couple of years, and that, in turn, makes it easier to prosecute.

I think that verifying Social Security numbers is a very interesting idea that potentially raises some privacy problems, depending on what records are being matched, that would give us some pause, but it is certainly worth exploring.

Senator CARPER. Thank you, and I recognize that. There has to be a public policy debate over those uses, between individual rights and the collective good. But I think it is a debate worth having.

I, too, endorse S. 2541 in the sense that under present laws now, a lot of sentencings in terms of identity theft are not as strong as they could be. We have had two recent investigations where the sentences, at least to a lay person, seemed light in view of the severity of the crimes that were committed. This is a bill that we really need soon.

Ms. FISHER. I would agree with that, Senator.

Senator CARPER. What else would you like to offer, Ms. Fisher?

Ms. FISHER. Well, I think this bill would increase the penalties which not only encourages our U.S. Attorneys across the country to prosecute these crimes, because there are harder sentences, but hopefully will have a significant deterrent affect when people want to steal others' Social Security numbers or other identification information to engage in bank fraud or credit card fraud or document fraud that relates to terrorism or anything else like that. So for the deterrent effect, as well, we think it is important.

Senator CARPER. Mr. Coombs.

Mr. COOMBS. I agree with Ms. Fisher. Any more tools that you can give law enforcement for their tool box is a tremendous enhancement. It is commonly known in criminal circles that the crime of identity theft, the penalties are low and the financial gains, the probability, are extremely high. S. 2541 has mandatory sentencing for identity theft, and if it is terrorism-related, there are more years added, and that is a tremendous bill and also would have the support of the Secret Service, as well.

In regards to information and verifying information, anything that we can do to verify businesses—verify information, because it really is the compromise of information that is the root cause of identity theft, and if there is any avenues to provide banking institutions, for instance, to verify information with good information versus the bad information that they are getting, that would be a tremendous asset to them.

I know the Treasury Department yesterday issued some regulations to enhance risk assessments and "know your customer" as a result of the PATRIOT Act, and the Secret Service works closely with the financial industry in developing protocols for knowing your customer. So, hopefully, with these protocols and enhancements and knowing your customers, we can do better at verifying this information.

Senator CARPER. Thanks.

Colonel STEVENS. I would like to take a little bit different approach, sir. I think the creditors, the banks, and the credit card companies, and the credit bureaus should be held accountable for opening fraud accounts. In my case, I have seen that just a little bit of diligence on checking an address, a birthdate, a place of employment—for instance, I was listed as working at Stanley Tools in Texas after I retired from Johns Hopkins University as a physicist, so——

Senator CARPER. How did you like working at Stanley Tools? [Laughter.]

Colonel STEVENS. It was enjoyable, apparently. The people spent a lot of money who worked there. But just to hold the people accountable to show a little bit of care in opening these accounts, look at birthdays, or a different address. Of course, I was told once that 15 percent of the people move every year, so they could not disqualify them for credit on that basis. My answer to that is, 85 percent of them do not move, so we all have to suffer for that.

Why can they not just take more care in opening the account, check the data, and the credit bureaus can look for any drastic changes. In fact, they have a protection policy now that costs, I think, $79.95 a year that they will do that. I thought they should do that under the normal process of doing business.

Senator CARPER. One follow-up question, and it sort of follows up to what Mr. Stevens has just said. When someone's identity is stolen and credit card purchases are made illegally using that stolen identity or other, whether it is credit card purchase or others, who ends up suffering the financial loss?

Colonel STEVENS. The creditor has to suffer that and that is why they are so determined that they are going to turn that account over to a third party collection agency, which comes right back on me. They will hound you to death to try to make you pay that bill. Now, some people will cave into that, and that is a warning to senior citizens like myself. Do not pay it, because that is an admission of guilt and that account will remain on your credit report, I believe, for 7 years. But they will hound you, they will call you on the phone, and if you clear it with them, they turn it over to another one, and we have had some recycled going on the fifth time now, with the same account.

Senator CARPER. What can we do to change the incentive so that the incentive falls more on the issuer of, we will say, the credit card to be more diligent in terms of the background checks to control their underwriting losses?

Mr. BEALES. Senator, I think, mostly, they have the right incentives now, because ultimately, it is the creditor that pays the losses and that is certainly the way it should be. If they issue credit to the wrong person, they ought to have to eat the loss.

The difficulty is, I think, from the creditor's perspective and also from the way the system as a whole has to work, is there are also people out there who do owe the money and simply are not paying. So creditors have a legitimate interest in trying to collect in those kinds of cases and it is hard for creditors to distinguish the victim of identity theft from the deadbeat in some cases.

We can try to make that process easier and encouraging people to file police reports is one thing that helps with that. We have developed a uniform fraud affidavit that creditors will accept as evidence that this really is an identity theft victim. But there is a tension there that is inherent in the nature of the crime that I think is difficult to get rid of entirely.

Mr. HUSE. This really comes down to the accuracy of these records, and that is the difficulty on the commercial side, is they have information that they have aggregated through various ways, but there is no way for them to verify that information in a facile way, or any obligation right now, either, other than due diligence in a business context.

If we make it, that cross-verification, a requirement, over time, the number has better standing than it does now. Right now, it is defeated because it is—the integrity is very amorphous, and I think that is really an aspect there that deserves a good look.

Senator CARPER. OK, good. You have been most helpful. Thank you for your testimony. Thank you for your response to our questions. Mr. Stevens, good luck.

Colonel STEVENS. As long the candle does not relight itself, we will be struggling out there. We are going to fight them, though.

Senator CARPER. Thank you.

Senator CRAIG. Tom, thank you very much.

Mr. Beales, one last question of you. Are there factors within the aging population that may indicate that this crime is being underreported relative to their general population, or relative to the general population. You were giving us statistics as to those victimized. In many other areas, we find seniors under report simply because of their view of their own personal integrity or their privacy sense or they are going to suffer through a bit of a different attitude in a population base compared to younger people.

Mr. BEALES. We certainly see that in our fraud cases, that the elderly are less likely to report that they are victims of fraud than are members of the population at large. It is not clear that translates here, although it may, because this is a little bit more like having your wallet stolen. This is to say you are a victim in a very different way than you are in a fraud where you sort of have to say you are a victim and you have to admit you were taken. But having your wallet stolen is not quite like that. So it is not clear that it is the same sort of a problem. It may be, and we are in the design stages of some research to try to find out whether there really is a difference, but at this point, we do not know.

Senator CRAIG. Alice, gentlemen, thank you all very much for your testimony today. You have helped build a valuable record. We appreciate it. Thank you.

Now, let me call our second panelists forward, if you would please come forward.

Let me thank our second panel for being here. Let us get started, if we could, please, and let me first introduce Mari Frank, a Privacy and Identity Theft Consultant from Laguna Niguel, CA. Mari, welcome before the committee.

STATEMENT OF MARI J. FRANK, ESQ., PRIVACY AND IDENTITY THEFT CONSULTANT, LAGUNA NIGUEL, CA

Ms. FRANK. Thank you very much, Senator Craig, for inviting me and for holding this important hearing. I am the author of the "Identity Theft Survival Kit," which I have brought as a resource to this committee to give to you.

Senator CRAIG. Great. Thank you.

Ms. FRANK. As a member of AARP myself, several years ago, an imposter took my identity and stole over $50,000 using my name and my profession as an attorney. Additionally, I have personally assisted hundreds of elderly victims myself.

There is very little that seniors can do to prevent this crime. Law enforcement needs more resources and it needs to investigate, which often they do not. But law enforcement will never have the power to prevent it. The key players with the unique opportunity to thwart this crime are governmental agencies and businesses that collect and use our information. Security breaches of databases, careless information handling practices, and unscrupulous employees facilitate this fraud. There is no control over information in the hands of others and there is no opportunity to avoid identity theft. Once victimized, it may take months or years to find out, and then to remedy the situation.

Here are a couple of examples of real-life stories. Sidney, a retired executive, learned that his identity was stolen after he and his wife purchased a new home. His loan application with his three-in-one credit report revealed his credit score, his Social Security number, and all of his accounts. His masquerader, using that loan application, was able to open new credit card accounts, rent a new apartment, obtain utilities, stealing over $100,000 in their name.

Allan and Marcia were retired in a mortgage-free home. They learned that convenience checks were stolen from their mailbox and thousands of dollars were spent in their name. Checks were stolen, credit cards were opened, other purchases were made. Worse yet, they learned that their mortgage-free home now had a mortgage with a lender who was threatening foreclosure.

Steve, a 78-year-old retired policeman, was living in an assisted care facility. His personal information was held in an unlocked cabinet in the nursing home and later used to purchase luxury cars and electronic equipment. He even found that he had a criminal and fraudulent DMV record in another State.

Lorraine, a 65-year-old widow of a deceased decorated United States Air Force General found out several months after her husband's death that his identity was stolen to commit security crimes. Not only is she left to deal with that grieving, but also to clean up his tarnished reputation.

Although Federal law protects victims of credit card fraud from paying the losses, as we know, there are still out-of-pocket costs, which may cost thousands of dollars. Also, for those who experience "ATM–VISA fraud," and check fraud, replacing the money in those accounts is almost impossible. Without assistance, the elderly feel overwhelmed, give up, pay fraudulent bills, or even file bankruptcy. Emotionally, seniors feel very victimized, and violated, not only by the criminal perpetrators, but even worse, by the creditors' harass-

ment and lack of cooperation, the frustration of the experience from the credit reporting agencies when they fail to correct, and the refusal of law enforcement to even investigate the crime.

The following factors make this crime easy and insidious: Mail theft; insider theft; dirty employees; unscrupulous relatives; hackers and high-tech fraudsters creating false documents; dumpster-diving at businesses and hospitals; information brokers selling personal information indiscriminately; selling of credit reports, loan documents, rental car applications; theft in offices, buildings, websites, computers; pretext calling and different scams; government and various industries' negligent information handling practices; public record access, including birth certificates and death certificates that have the Social Security number.

It is a myth that seniors can prevent identity theft. Offering consumer tips like ordering your credit reports twice yearly and guarding your personal information and shredding are great information, but gives our aging population a sense of false security. Precautions taken by government entities and private industries should do the following, and by the way, I have 17 pages in my written testimony to give many more things, but I will just give you a few.

Senator CRAIG. Thank you. [Laughter.]

Ms. FRANK. Because you were asking for solutions on the last panel, I have bullet pointed all the things that we think should be done.

Limit the use of the Social Security number, since it is the key to identity theft. Verify, authenticate, and protect whatever identifier is used, whether it is a number, a password, or biometric information. Completely destroy personal information that companies are discarding. They should truncate credit card numbers and other unique identifiers, like Social Security numbers, and secure all data, online and offline, and they should notify customers and consumers or employees of security breaches.

Rather than going any further, I just want to end with whether a Social Security number or a biometric identifier is used, the same issues arise. How will we protect that information as it is stored, transferred, sold, or used? Our nation's aging population, the fastest growing segment of our society, is most at risk to be victimized by the fastest growing crime. Let us set realistic guidelines for information handling practices. Thank you.

Senator CRAIG. Mari, your testimony is valuable and I think those examples and recommendations based on your experience are extremely valuable and I thank you for that.

[The prepared statement of Ms. Frank follows:]

TESTIMONY FOR THE UNITED STATES SENATE

SPECIAL COMMITTEE ON AGING

SENATOR JOHN BREAUX, CHAIRMAN
LARRY E. CRAIG, RANKING MEMBER

SENATE'S SPECIAL COMMITTEE ON AGING
INVESTIGATIVE HEARING ON IDENTITY THEFT
HEARING DATE: JULY 18, 2002 9:30A.M.
ROOM SD-628
DIXON SENATE OFFICE BUILDING
TESTIMONY PROVIDED BY MARI J. FRANK, ESQ.

Good morning, Chairman Breaux, Ranking Member Craig, honorable committee members, and invited guests. Thank you very much for the opportunity to address you today regarding this hearing on Identity Theft and the vulnerability of senior citizens to this crime.

My name is Mari Frank. I am an attorney, privacy and identity theft consultant, and author of the Identity Theft Survival Kit (Porpoise Press, 1998) from Laguna Niguel, California. I serve as a Sheriff Reserve (Professional Services) for the Orange County, California Sheriff Department's High Tech Crime Unit, and sit on the Advisory Committee to the Office of Privacy in the State of California's Office of Consumer Affairs, which focuses on privacy and identity theft protection for California citizens. Additionally, I have served on the Los Angeles District Attorney's Office Task Force on Identity Theft, which sponsored legislation to help victims of identity theft, and assisted law enforcement in the prosecution of this crime. As an advisory board member to the non- profit consumer advocacy program, the Privacy Rights Clearinghouse (San Diego, Ca.), I am privileged to consult with Director Beth Givens and Linda Foley (Director of the Identity Theft Resource Center- an affiliate program) regarding identity theft cases and proposals for legislation.

My own identity was stolen (in 1996) by an impostor who paraded as an attorney and took over $50,000 in my name. From that arduous nightmare, I gained great insight into the tribulations that victims endure. Since that time I have personally assisted myriad victims, many of who are between the ages of 50 and 93 years old. Additionally, I have had the privilege of testifying before several legislative bodies and have advised many national corporations on how to protect their clients, customers, vendors and employees and their company from problems of identity theft.

First I am grateful to this honorable committee for focusing on the growing problem of Identity Theft with regard to our aging population. Your desire to expose the scope of its prevalence and its causes deserves commendation. I am also thankful to this esteemed panel of witnesses who will assist you in creating solutions to the unique challenges of dealing with this white-collar crime.

You've asked that I concentrate my testimony in the following areas:

I. Explain the vulnerability of seniors to identity theft, and provide brief case histories.
II. Describe the financial and emotional impact on senior victims of Identity Theft.
III. Clarify what seniors **can** and **cannot** do to avoid Identity Theft.
IV. Propose actions that private sector and government should take to protect seniors from becoming victims of Identity Theft.

I. THE VULNERABILITY OF SENIORS TO IDENTITY THEFT

To understand the unique problems facing the aging with regard to identity theft, I will clarify what actually happens to victims. There are many types of fraud that fall under the category of identity theft. It could be as simple as "account take over" where the thief steals an ATM VISA or MasterCard, credit card, or just the account number, and makes purchases on-line, by phone or in person. By stealing your mail or trash, a fraudster can either use your checks or create new checks using your account number to drain the funds from your bank accounts. You only find out when your checks start bouncing or you can't use your ATM to obtain cash.

Fraudulent purchases can also be made without your knowledge if your credit cards are "skimmed". A "dirty employee" at a retail store, restaurant, or hotel simply duplicates the metal strip on the back of your credit card using a skimmer (a small handheld device designed to copy information from the magnetic strip on a card) to later create a new card with your account information- thus your credit card bill arrives normally with purchases you never made- yet your credit card sits safely in your wallet.

The more invasive and lucrative type of identity theft- "true name fraud" or "application fraud" occurs when your "evil twin" obtains your social security number, (that's often all they need) pretends to be you, and applies for credit at his/her address or a mail drop. The thief, needing a photo ID, obtains a driver's license- either a "valid" duplicate from the state Department of Motor Vehicles (many states are less than careful in issuing duplicate licenses, i.e.: California issued over 100,000 duplicate "valid" licenses with the impostor's photo to fraudsters in the year 2000), or buys a high tech phony license on the street for $25.00. With just these documents, the "identity clone" can create havoc in your life. The impostor can obtain more credit cards, credit lines, a mortgage, an apartment, purchase cars, open utilities accounts, get a cellular phone, make cash advances, obtain health care, purchase life insurance in the victim's name, (making the fraudster the beneficiary), order a passport, work under your name (and of course the IRS comes after you), become a "legal" citizen, steal your professional identity (even create business cards), create e-mail accounts and web sites, and worse yet, commit crimes ruining your good name and destroying your reputation.

Although every one of us is vulnerable to this crime (since our personal information including our social security number is readily available offline and on line and its use, sale and transfer is often beyond our control), seniors are a more susceptible for a variety of reasons:

1. Seniors Place Value on Creditworthiness and Owning a Mortgage-Free Home

Typically, seniors establish a more conservative financial profile as they get older. Many have acquired wealth, a home, financial stability and a better credit score than younger

people. A savvy identity thief can access and be extended more credit for purchases for a longer period of time if they target an older person with higher credit line availability.

Sidney, a wealthy retired executive learned that his identity was stolen many months after he and his wife purchased a new home. His loan application, with his 3 in one credit report attached, revealed his credit score, his checking, savings, and investment accounts, social security number, and all necessary information for an impostor to become Sidney. His masquerader had gotten a copy of Sidney's loan application and opened new credit card accounts, purchased computers, electronic equipment, furniture, rented an apartment, obtained utilities, etc, stealing almost $100,000.

Allan and Marcia are retired and living in a gate guarded community, in a mortgage free home. They felt sure that their mail and finances would be safe inside the gate, yet they learned that convenience checks were stolen from their mail box, and thousands of dollars were spent in their name. Also their own checks were stolen, credit cards were opened in their name, purchases were made across the country using their credit card numbers on the Internet. After several months, they learned that their "mortgage-free" home now had a large mortgage and a lender was threatening forclosure.

2. Seniors At Risk for Pre-text Calling

Elderly persons who are weak or ill may be prone to deceptive approaches such as pre-text calling which is a method that a fraudster can use to extract personal information to then use to steal from the victim.

David a 70-year-old diabetic from Detroit had received a call at 10:00 PM one evening supposedly from the local court system telling him it was time to serve on jury duty. They required his social security number, birth date and other personal information Fearful of repercussions: he answered all the questions posed to him. He never received any call for jury duty, but he did receive calls from collection agencies several months later regarding new credit accounts that he hadn't opened.

3. Many Seniors Dependent on Caregivers

Nursing homes and Board and Care Home employees as well as in-home caregivers are often placed in a tempting situation where they have access to personal information and they are in a position of trust. Very ill seniors, especially those with Alzheimer's and other disabilities often are at the mercy of the caregiver to help them with banking, health care information (which usually includes the social security number) and even Living Trusts and insurance. Here's an example:

Mary, a 70 year old blind woman, was living with her adult son who hired a practical nurse to help his mother while he was at work. The nurse's aid took Mary to doctors' appointments, the bank, and also to the cleaners –literally and figuratively- she stole Mary's identity using her social security number to obtain credit cards, utilities, a new car, and an apartment and even left Mary with a warrant for unpaid parking tickets. The family didn't learn of the theft until the caregiver was nowhere to be found.

4. Older Americans Lack Emotional Energy to Deal with Overwhelming Issues of ID Theft

Addressing the issues of regaining one's financial creditworthiness is very challenging for anyone, but the elderly are especially vulnerable when they live alone or have experienced the loss of their spouse after many years of marriage.

Loraine, a 65 year old widow of a deceased decorated United States Air Force General, found out several months after her husband's death that his identity was stolen to commit security crimes and credit card fraud. Not only is she left to deal with her grieving, but also the tremendous burden of repairing her husband's tarnished reputation and addressing her own financial disaster of trying to convince the collection agencies that the debts didn't belong to her late husband. Although her identity wasn't stolen she became the victim.

5. Health Challenges Exacerbate Problems- especially with Criminal ID Theft

George, a 55 year old disabled veteran living in Colorado was suddenly denied his disability payments, and hit with a large IRS bill for the income that his impostor had earned working under his name in Tennessee. Upon investigation, we learned that George's impostor had also established a criminal record in yet another state and there was a warrant for George's arrest.

Delores, 62, takes kidney dialysis treatment three times a week at a hospital clinic near her home. She learned that she and several other patients had their identities stolen by an employee who had access to their personal information. She has no financial resources and no children to help her. She feels lost and terrified.

6. The Elderly Victimized by their Children or Relatives - Fearful of Law Enforcement

Sadly some unscrupulous relatives, like vultures, take advantage of the finances and good nature of their family. They bank on the fact that the victims won't go to the police telling the

truth about the fraudulent use of their identity and credit. This hinders law enforcement and may cause the victims' reputation to be ruined.

John Sr. a 75-year-old retired engineer learned that John Jr. had been using dad's credit to make purchases and buy a car. Rather than turn in his son, John Sr. made payments for years to the various companies until he found out that Junior had also taken a second mortgage on his parents' home. He is fearful of losing his home and doesn't want to put his son in jail. His health is failing and his heart is breaking.

7. The Information Age, lightening speed data transfer, and technology overwhelm seniors

Our aging population has had to adjust to the information age- new technologies, which are challenging to grasp for those who grew up with typewriters. For many elderly persons, it is just too overwhelming to get help on the Internet, protect themselves on-line or understand all the precautions to take on the Internet.

Susan, a 60ish hip grandma, signed up for e-mail and Internet access with a reputable Internet Service Provider. When she received e-mail from her provider asking her to give her personally identifying information, including her social security number, to renew her account, she found out that it was a ploy by hackers to get her information. It was a false e-mail set up to look like her provider. She later became the victim of identity Theft with thousands of dollars worth of purchases on the Internet with credit cards she didn't know she had.

The above cases caused great anguish to the victims who called us. The time spent trying to regain their lives and the out of pocket costs were minimal compared to the tremendous emotional turmoil these seniors experience.

II. FINANCIAL AND EMOTIONAL IMPACT ON SENIOR VICTIMS OF IDENTITY THEFT

1. Financial Aspects:

Most seniors who are victims of credit card fraud are protected by federal law with regard to the fraudulent charges, however for those who experience ATM VISA and MasterCard fraud and check fraud, regaining the money into their checking account has been far more challenging and many victims find they cannot handle the issue without the help of legal counsel. This of course is an out of pocket cost. Additionally, sending letters return receipt requested, hiring help to type the letters, long distance phone calls, missing time from work, doctor bills from increased health problems, credit monitoring services, private investigators, notary fees, and attorney fees all increase the out of pocket costs expenses. Further research among senior victims will be necessary to assess the true financial devastation. My experience hearing from the elderly is that if they don't have family members to help them make the calls and write the letters, and they cannot afford an attorney, they feel

overwhelmed, give up and pay bills that are fraudulent. Some have reported that they resorted to bankruptcy since they felt they had no other choice.

In May of 2000, Calpirg and The Privacy Rights Clearinghouse issued a report entitled "Nowhere to Turn: Victims Speak Out on Identity Theft". The victims in that study (although not specifically over 50 years of age) reported an **average** of 175 hours and $808 in out of pocket costs – but only 45% of the victims included in the averaged costs considered their cases to be solved. 55% of those surveyed whose cases were still open reported that their cases had already been open almost 4 years. Victims reported spending between $30 and $2000 **not** including attorney fees. (See www.privacyrights.org/ar/idtheft2000.htm for complete report)

II. The Emotional and Psychological Impact on Aging Victims of ID Theft

Victims feel extremely violated by the criminal perpetrator, but even worse, the victims often experience blame and disbelief by the creditors, lack of cooperation and concern by the credit reporting agencies, and refusal by law enforcement to investigate.

Victims often report that creditors demand payment, and treat the victim like a deadbeat. Credit card companies and banks normally refuse to provide documentation of the billing statements and applications, and may sell the "delinquent" accounts to collection agencies even after fraud is reported. Then the collection agencies hound victims, threatening lawsuits.

Victims report great difficulty in contacting the credit reporting agencies since there are no live persons to assist them upon reporting the fraud. Also reading the credit reports and understanding them causes great frustration since all three companies use different formats. Confusion also occurs since the credit report that the consumer receives is different from the one that the creditor receives. Even after a fraud alert is placed on the credit profile, victims feel insecure because careless creditors will issue new fraud accounts without any negative consequences for the creditor or the credit reporting agencies. Many victims also report that once fraudulent activity is removed from the credit report it may reappear on subsequent reports without re-reporting from the creditor. Cleaning up the credit mess may take months or years.

Although most state and federal law ensures that consumer victims have standing to make at least an informational police report in the jurisdiction where they live, many law enforcement offices still refuse to issue a report and most victims find that unless there is a suspected fraud ring or a very high dollar loss, there will be no investigation. If there is no inquiry, the impostor can strike again- leaving the victim feeling terrified. Hurdle after hurdle causes feelings of dread, rage and fear.

Identity Theft is a frightening and overwhelming experience for anyone at any age, however for our older citizens it is often compounded by health challenges and other vulnerabilities unique to the elderly. This crime is like a cancer in that it strikes without warning and

disrupts your whole life-it may go into remission, but you don't know when it will strike again, especially if the impostor isn't caught. In only 10% of the cases is there an arrest.

The elderly victims with whom I have personally spoken and those that report to the Privacy Rights Clearinghouse and the Identity Theft Resource Center all have very similar feelings of frustration, violation, fear, helplessness, anger, rage, anguish, powerlessness, and even despair. Victims feel out of control since most do not know who is doing this to them, why this is happening and they just can't stop it. Those who experience this crime, like victims of violent crime also experience posttraumatic stress disorder- they report they are unable to sleep, extreme loss or gain of weight, feelings of isolation, paranoia, intense distrust and even embarrassment that someone will think that because this happened to them that they are old and incompetent

The negative psychological response may even cause physiological reactions and physical manifestations-the stress and anxiety have caused heart palpitations (one of our victims had a heart attack), high blood pressure, back and neck spasms, shortness of breath, stomach upsets, headaches, eczema, sexual dysfunction, depression, and night terrors. One distraught law enforcement fraud investigator in South Florida called me to tell me that one of his elderly victims committed suicide from the extreme depression she experienced from dealing with her "identity theft hell".

Without intervention, many of the elderly seniors could be in great psychological danger. We recommend emotional counseling services, but encourage the development of strong victim assistance programs to provide support groups and therapy.

III. WHAT SENIOR CITIZENS CAN AND CANNOT DO TO PROTECT THEMSELVES FROM IDENTITY THEFT

We've heard numerous identity theft stories- with numbers of victims ranging from 500,000 to over a million a year. In the year 2001 Trans Union, one of the three major credit reporting agencies, reported an average of 3,500 calls a day to their fraud hotline. Some of those reporting had lost their wallets or their information was stolen and they had not yet become victims, so we are not sure of how many of those became victims, however the number is significant. Our current statistics from the Federal Trade Commission do not reflect the true extent of Identity Theft, because most victims still do not know to report to that entity- the credit reporting agencies are still in the best position to share the statistics that they have with the FTC and should be required to do so to assist in adequate research.

What can elderly victims do to protect themselves? Under current law, they have very little control how their personal information is disseminated or accessed, but they can do simple common sense things to **minimize their risk-**

Here are the top four protection measures:

1. Get a copy of your credit reports at least twice a year. Carefully scrutinize all information and correct all errors, including the inquiries. If something looks strange, call and write to the creditor and place fraud alerts on the credit profiles of the three major credit reporting agencies. If you monitor your reports and fraud accounts are opened, at least you will minimize your losses with early notification. Do your own background search on yourself once a year to see if any fraudulent criminal activity appears.

2. Don't give out your social security number unless required by law. Don't carry it with you and if it is on your health care cards, make a copy redacting the first 5 numbers and carry only the copy with you. Carry as little information about you as possible in your wallet. Don't submit to the use of your biometric information (fingerprint, iris scan, etc) unless required by law and you understand the purpose for which it is collected, how it will be maintained, the secondary use if any, the safeguards ensuring its accuracy and security and the place to contact if a problem arises.

3. Guard your personal information with great caution. Don't give out information at retail stores, on warranty cards, when a company *calls you* on the phone, or on the Internet. Don't keep personal information on your computer if it is accessible on the Internet. Shred all documents that you are discarding, including utility bills, check statements, old wills and trusts, ***anything*** with personal and financial information.

4. When dealing with others in a trusted position, such as a caregiver, or a trusted advisor, make sure you check references, licenses, and other background information. Share as little personal and financial data with this person as possible, and don't give them responsibility to manage your assets without your approval- don't give out your ATM VISA pin number or allow them to sign checks for you. The less access to your financial and personal data the more secure your identity.

CAUTION- INFORMATION ACCESS BEYOND YOUR CONTROL- MAJOR CAUSE OF IDENTITY THEFT

Even if you diligently take every precaution delineated on informative web sites such as www.identitytheft.org; or www.privacyrights.org or www.idtheftcenter.org or the FTC website at www.consumer.gov/idtheft and *all* the other websites that repeat the *same advice*, you are still **very vulnerable** to becoming a victim of identity theft given the present situation where consumers have no control over limiting access to personal information. With the tools below, someone can easily masquerade as you and destroy your good name.

1. **Mail Theft-** although you can minimize your risk with outgoing mail by placing your checks and payments in the box at the post office and not your own mailbox, you have no control over insider mail theft by employees, by thieves stealing from mail trucks, post offices, or from those with whom you do business.

2. **Insider- dirty employees, unscrupulous relatives-** workplace identity theft is an epidemic. Your information is stored in your doctor's office, your accountant's office,

hospitals, nursing homes, dental offices, credit card companies, credit reporting agencies, the IRS, banks, investment companies, mortgage brokers, etc. You have **no idea** who has access to that information and what they may do with it illegally.

3. **Hackers-**whether or not you use the Internet, your personal information may be sitting on a computer or a web site and without your knowledge a hacker may get access to that information and sell it for fraud purposes.

4. **Dumpster Diving-** Even if you shred all your personal and financial information, you have no control what governmental and commercial entities are doing with your sensitive information when they discard it. California and Wisconsin have laws, which require complete destruction by commercial companies when discarding personal information. This should be federal law and it should also to governmental agencies as well.

5. **Information Brokers-**Private investigators and on–line brokers, who are not under strict scrutiny, gather information about you from various data bases and re-sell that information-even your social security number. For a price, you can order almost any information you wish about anyone. With the information obtained one can easily steal another's identity.

6. **Obtaining Your Credit Report**-many businesses have subscription services with the credit reporting agencies (real estate offices, attorney offices, lenders, credit card companies, etc.) Someone can allege that they have a permissible purpose to obtain your credit report and have all the information needed to assume your identity.

7.**Burglary at office buildings, hospitals your home, your car, etc.**
A burglar at your bank, an employer, former employer, a former friend or estranged or disloyal family member, roommates or employees at your home could all steal enough information to become your "evil twin".

8. **Pretext Calling-**
Someone intending to get information about you may call your employer, doctor, investment office, or even your friends or family to gain information to steal your identity.

9. **Credit Industry Carelessness**
Credit grantors facilitate this crime by issuing credit far too easily. Billions of pre-approved offers are sent each year without prior consent (a report by the New York Times reported 11 Billion pre-approved offers for credit in the year 1999) as are "convenience checks" that can easily be cashed by an impostor.

Many creditors issue credit to impostors even after fraud alerts are posted on the credit profile. In their zeal to issue quick credit, credit card companies fail to match names, addresses and other information to verify identity when issuing credit lines and credit cards.

10. **Public Record Access**

Birth Certificates and especially death certificates make identity theft very easy. A death certificate has the social security number of the deceased. In fact when Kevin Mitnick, the famous hacker, called to interview me about identity theft (for his radio show) he personally told me he committed identity theft by stealing the death certificates of young children. Then he could hide out and work under the assumed names, get credit cards, apartments and all he needed.

The Myth of Prevention of Identity Theft

The points above are just a few of the ways that your information can be accessed and used for a criminal purpose without your knowledge or control. When I became a victim, my impostor had accessed my credit report from a law office when she pretended to be a private detective who allegedly had a permissible purpose, I had no way to prevent this crime from happening.

Giving senior citizens tips on how to "avoid" identity theft is misleading. Although we may educate them to stay conscious and guard their information as best as possible, I urge this committee to take notice that we should **not** give any false sense of security to anyone with regard to identity theft. There are steps that could be taken to prevent financial identity theft that I will address in my section on "proposed actions to be taken by the private sector and government."

Clearly, the elderly need to be educated to understand how to minimize the dissemination of their information, but they should also understand that they must demand accountability by the various industries that have collected their information. Hopefully, we can collaborate with the financial industry, governmental entities and all businesses, to see how secure information handling practices and respect for privacy is a value added to enhance trust with seniors.

IV. PROPOSED ACTIONS FOR THE GOVERNMENT AND PRIVATE INDUSTRY TO PREVENT SENIORS FROM BECOMING VICTIMS OF IDENTITY THEFT

1. Both governmental entities and private industry should limit the use of the social security number since it is the key to identity theft for financial fraud.

As a member of the advisory committee in the Office of Privacy Protection in the California Office of Consumer Affairs, I had the privilege of assisting in the development of the recently issued " Recommended Practices for Protecting the Confidentiality of Social Security numbers" (July 25, 2002 www.privacy.ca.gov). The following should be considered by both pubic and private sector entities to protect all consumers. These provisions are especially beneficial for the protection of seniors.

Recommended Practices for Protecting the Confidentiality of SSNs by the Office of Privacy Protection of the California Office of Consumer Affairs

The Office of Privacy Protection's recommendations are intended to serve as guidelines to assist organizations in moving towards the goal of aligning their practices with the widely

accepted fair information practice principles described below. These recommended practices address, but are not limited to, the provisions of California Civil Code section 1798.85.

The recommendations are relevant for private- and public sector organizations, and they apply to the handling of all SSNs in the possession of an organization: those of customers, employees and business partners.

1. Reduce the collection of SSNs.
   Fair Information Practice Principles: Collection Limitation, Use Limitation

- Collect SSNs preferably only where required to do so by federal or state law.
- When collecting SSNs as allowed, but not required, by law, do so only as **reasonably** necessary for the proper administration of lawful business activities.
- If a unique personal identifier is needed, develop your own as a substitute for the SSN.

2. Inform individuals when you request their SSNs.
   Fair Information Practice Principle: Openness, Purpose Specification

- Whenever you collect SSNs as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, whether the law requires the number to be provided or not, and the consequences of not providing the number.
- If required by law, notify individuals (customers, employees, business partners, etc) annually of their right to request that you do not post or publicly display their SSN or do any of the other things prohibited in Civil Code Section 1798.85(a). Eliminate public display of SSNs.

3. *Fair Information Practice Principle: Security*

- Do not put SSNs on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, bulletin board postings, and other materials.
- Do not send documents with SSNs on them through the mail, except on applications or forms or when required by law[i].
- When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.
- Do not send SSNs by email unless the connection is secure or the SSN is encrypted.
- Do not require an individual to send his or her SSN over the Internet or by email, unless the connection is secure or the SSN is encrypted.
- Do not require individuals to use SSNs as passwords or codes for access to Internet web sites or other services. Control access to SSNs.

  Fair Information Practice Principle: Security

- Limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.
- Use logs or electronic audit trails to monitor employees' access to records with SSNs.
- Protect records containing SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
- Do not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
- Avoid sharing SSNs with other companies or organizations except where required by law.
- If you do share SSNs with other companies or organizations, including contractors, use written agreements to protect their confidentiality.
- Prohibit such third parties from re-disclosing SSNs, except as required by law.
- Require such third parties to use effective security controls on record systems containing SSNs.
- Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.
- If SSNs are disclosed inappropriately and the individuals whose SSNs were disclosed are put at risk of identity theft or other harm, promptly notify the individuals potentially affected.
- Protect SSNs with security safeguards.

Fair Information Practice Principle: Security

- Develop a written security plan for record systems that contain SSNs.
- Develop written policies for protecting the confidentiality of SSNs, including but not limited to the following:
- Adopt "clean desk/work area" policy requiring employees to properly secure records containing SSNs.
- Do not leave voice mail messages containing SSNs and if you must send an SSN by fax, take special measures to ensure confidentiality.
- Require employees to ask individuals (employees, customers, etc.) for identifiers other than the SSN when looking up records for the individual.
- Require employees to promptly report any inappropriate disclosure or loss of records containing SSNs to their supervisors or to the organization's privacy officer.
- When discarding or destroying records in any medium containing SSNs, do so in a way that protects their confidentiality, such as shredding.[ii]
- Make your organization accountable for protecting SSNs.

Fair Information Practice Principle: Accountability

- Provide training and written material for employees on their responsibilities in handling SSNs.
- Conduct training at least annually.

- Train all new employees, temporary employees and contract employees.
- Impose discipline on employees for non-compliance with organizational policies and practices for protecting SSNs.
- Conduct risk assessments and regular audits of record systems containing SSNs.
- Designate someone in the organization as responsible for ensuring compliance with policies and procedures for protecting SSNs.

2. **Destruction of Confidential Information**-Governmental Agencies and Private Industry should be required to completely destroy personal information that they are discarding by shredding, burning or whatever means is necessary to protect the information from dumpster diving.

3. **Governmental and Private industry should be required to truncate credit card numbers** – No company or entity shall print more than the last 5 digits of a credit card number or account number or the expiration date upon any receipt provided to a cardholder.

4. **Security Breach Notification** Governmental Agencies and Private industry should be held accountable to timely notify all employees and or clients or customers of computer security breaches which have exposed their personal identifying information.

5. **Departments of Motor Vehicle Licensing-** Bureaus should establish more stringent monitoring and matching of duplicate licensing and new licenses. A photo ID and a fingerprint could be matched. Rather than developing a "national ID" with various forms of biometric information, credit cards and other unnecessary information which would complicate the process, this national driver's license would have a national data base to help deter interstate identity theft.

6. **Law enforcement agencies** should be required to take a report in the jurisdiction where the identity theft victim lives. Such report should enable the victim to list the fraudulent accounts so that this report could be sent to the credit reporting agencies to comply with their policy of blocking the fraud accounts upon receipt of a valid law enforcement report.

7 **Law enforcement agencies** should be provided funding for task forces in all major metropolitan areas to include the Secret Service, the Postal Inspector, the Social Security Inspector, the FBI, INS, State Attorney General and local law enforcement to collaborate in the investigation and prosecution of these crimes.

8. **Local law enforcement agencies** in conjunction with the judicial system should assist victims of criminal identity theft in other jurisdictions within a nation wide coordinated system. So a victim of criminal identity theft in California whose impostor is in New York could be declared innocent in New York as well as California. This would entail a national database of the criminal information and fingerprints. It would contain the order of the true

person's fingerprints for comparison with the fingerprints of the impostor-criminal in New York. The court would enter a declaration of factual innocence and any warrants for the victim would be dismissed. All databases would be corrected so that background checks would not show the victim as having an arrest or criminal record.

9. Increase penalties for repeat identity theft perpetrators or for "aggravated identity theft" and for those who commit identity theft for the purpose of committing terrorism.

10. Set up State and Federal Offices for Privacy Protection- There should be a federal office of privacy protection as well as state offices. The office of privacy protection should institute an ombudsmen office to assist the elderly and limited English speakers to resolve identity theft problems.

9. Credit Reporting Agencies:

a. Since most victims do not have notice of the identity theft until they re-finance, apply for a loan, or are contacted by a creditor, the statute of limitations to file a law suit against a credit reporting agency should begin within 2 years of the date at which they discovered or should have known of the fraud.

b. To assist in the monitoring of credit reports, consumers should be entitled to a free credit report at least once a year in every state.

c. Credit reporting agencies should provide to consumers, upon request, an exact copy of the credit reports that vendors and creditors receive since often they are different and the consumer credit report often shows different account information, which causes difficulties for victims in clearing their credit.

d. Consumers should be able to put a complete freeze on their credit reports in order to prevent identity theft. This would enable the consumer to prevent their credit report from being accessed by a creditor without the specific authorization of release. It would be impossible for an impostor to apply for credit if there were a freeze on the file. The consumer would have the right to release the file when he so desires by a password or pin number. This type of legislation recently became law in California.

e. Credit reporting agencies should be required by law to block all fraud including the fraudulent inquiries upon the receipt of a valid law enforcement report (local police, DMV investigators, Secret Service) listing the fraud accounts. The burden then shifts to the creditors to prove that the accounts are not fraudulent. This is presently law in California and should be codified nationwide. Under this scenario the victim of fraud is innocent until proven guilty instead of having the burden of proving innocence.

f. Credit reporting agencies should provide names, addresses and phone numbers of the companies who accessed the consumer's credit report –(inquiries) with the issuance of a consumer report so that potential victims could verify the permissible purpose.

g. Credit reporting agencies should notify a consumer by e-mail or First Class mail when his/her credit report has been accessed. The agency should be allowed to charge a reasonable fee for this service.

h. Amend the Fair Credit Reporting act to allow for class action lawsuits for violations of the act by creditors and credit reporting agencies.

i. Credit reporting agencies should set up hotlines with live persons to talk to regarding identity theft. The same employee in the fraud department should be assigned to a particular victim.

10. Creditors should be held accountable for protecting seniors and others from identity theft.

a. The fraudsters' most critical need in committing identity theft is to change the victim's address to the impostor's address or mail drop. Creditors either extending credit to a new account or upon being asked to change the address on the account be required to verify the address change if it is different from the address on its records or the address on the credit report. The creditor should be required to send a notification and confirmation to the former as well as the new address. Also if the creditor receives a request for an additional card it should notify the primary cardholder.

b. Creditor's who issue credit to an impostor after a fraud alert is placed on a credit profile, should be held liable and assessed a fixed penalty of at least $1000 per occurrence or actual damages which ever is greater.

c. Upon receiving notification of fraud by a victim of identity theft, a creditor should be required within 15 days to provide copies of all billing statements, applications and other correspondence to the victim. The victim may be required to pay reasonable copying costs.

d. Credit grantors should compare and match with the credit report for verification purposes, at least four pieces of personal information that would identify a consumer applying for credit.

e. Credit grantors should utilize their financial discrimination programs to identify changes in spending habits so they could intervene early and notify consumers of possible fraudulent activity before it gets out of hand.

f. Creditors should not be allowed to send "convenience checks" without a request by the consumer.

g. Credit grantors should not be allowed to send pre-approved offers of credit without the request of the consumer.

11. Information Brokers

a. Information brokers should be subject to the Fair Credit Reporting Act as defined by statute so as not to shirk their duty to maintain accurate records.

b. Employers or others who order background checks on a consumer should be required to provide a copy to the consumer upon receipt whether or not the consumer report was used to hire a prospective employee or any other purpose.

Summary of Problem:

We are living in an easy credit society where information is readily transferred across the nation in a nano-second on the Internet. Our personal information, worth more than currency, can be used to apply for numerous credit cards on-line without our knowledge. The fraudster can do anything we can do and even things we wouldn't do like commit crimes or terrorist activities. Our nation's aging population, the fastest growing segment of our society, is most at risk to be victimized by the fastest growing crime of our time.

We must address this problem on a national level to work collaboratively among all stakeholders to protect our vulnerable seniors and all consumers. With the ease of movement and communication, a retired veteran in Chicago may have an impostor in New York City who then sells the data to another criminal in Miami who in turn sells the information to a fraud ring who intends to sells credit cards to terrorists. These problems are complex, perplexing and overwhelming for the victims and our country. Governmental agencies and all businesses must be conscientious concerning the verification of identity, more cautious about confirmation of address changes, diligent about respecting the privacy and confidentiality of everyone's information, and enforce proper safeguards against unauthorized access. When we all work together to enhance privacy protection, our aging

population will be less susceptible to identity theft, law enforcement will be able to focus on reducing violent crime, and the financial industry will save billions of dollars.

Thank you for your time and efforts on behalf of our senior citizens.
Mari Frank

Senator CRAIG. Now, let me turn to Boris Melnikoff. Boris is the Consultant to the Regional President of the American Bankers Association, Atlanta, GA, and I understand has just become the grandfather of a ninth granddaughter, is that correct, Boris?

Mr. MELNIKOFF. That is correct. Thank you very much, Senator.

Senator CRAIG. Congratulations.

Mr. MELNIKOFF. Thank you, sir.

Senator CRAIG. Those are special things in one's life.

Mr. MELNIKOFF. At 1:57 yesterday afternoon, sir.

Senator CRAIG. Congratulations. Please proceed, Boris.

STATEMENT OF BORIS F. MELNIKOFF, CONSULTANT TO THE REGIONAL PRESIDENT, AMERICAN BANKERS ASSOCIATION (ABA), ATLANTA, GA

Mr. MELNIKOFF. Thank you, sir. Stopping identity theft before it occurs and resolving those unfortunate cases that do occur is of the utmost importance to the banking industry. Banks have a long, proud history of securing their customers' information, including those of senior citizens.

As technology and the Internet have made more information readily available, we have redoubled our efforts to help educate consumers about how to prevent and resolve identity theft. Banks and our customers are partners in protecting information.

This morning, I would like to make three key points. First, the banking industry has been actively involved in an ongoing effort to educate consumers on how to protect themselves from identity thefts. Each one of us can limit vulnerabilities to this crime.

Second, the American Bankers Association has developed videos, articles, statement stuffers to assist in training bank staff and educate consumers.

Third, it is important for the private and public sectors to pursue innovations to improve identification of individuals, beginning, for example, with the improved standards for drivers' licenses.

Identity theft harms consumers and banks and severely challenges law enforcement. We can only be successful in fighting this crime if we all work together. In 1998, ABA was very supportive of the changes made by Congress, led by Senator Kyl, which made it easier for law enforcement to bring action on ID theft cases. Unfortunately, at that time, there was no appreciable increase in prosecutions, however, likely due to the high volume of cases that law enforcement was already engaged in. We were encouraged, however, by the Justice Department's announcement in May that a nationwide effort has resulted in 73 criminal prosecutions for identity theft.

Let me now turn to the educational efforts of the industry. ABA members have been leaders in the private sector's push to educate consumers. We realize that people need our expertise and guidance to avoid being victimized. Of course, the first step to combat identity theft is self-awareness and how you can protect yourself. I have included in my written statements tips on protecting one's personal information. Taking many small steps, while not eliminating identity theft, will diminish the frequency of the crime.

Let me highlight a few examples of what the ABA has done. Just yesterday, I did a radio tour where I was interviewed on 15 radio

stations from coast to coast talking about ID theft prevention. These stations collectively reached an estimated 9.5 million listeners.

Second, the ABA has distributed to all its members a theft communication kit. This kit contains, Senator, public service announcements, sample statement stuffers, sample newspaper columns that a banker could tailor to his or her community. We have provided a copy of this kit to the committee.

Senator CRAIG. Thank you.

Mr. MELNIKOFF. ABA also offers a separate statement stuffer for banks to use in mailing to consumers, with close to six million distributed across the country already.

Finally, the ABA has sent 1,200 copies of a video produced by JP Morgan Chase and Company to our members. A copy of the tape has also been supplied to the committee, sir.

While the ABA has done a considerable amount of work in this area, we realize the individual industry efforts must continue. Fortunately, many of our members are engaged in similar efforts across the country. I continue to witness superb examples of industry's outreach, many of which I have mentioned in my statement.

Mr. Chairman, the ABA urges government leadership directed at improving methods of identifying individuals. There is no better way to protect against fraud and terrorism than by improving the identification documents used to complete financial transactions. Specifically, we believe in the efforts to improve how States issue drivers' licenses is of particular importance.

Thank you for the opportunity to update the committee on the industry efforts in this important area.

Senator CRAIG. Thank you.

[The prepared statement of Mr. Melnikoff follows:]

Testimony of
Boris F. Melnikoff
On Behalf of the
American Bankers Association
Before the
Special Committee on Aging
United States Senate
On
Identity Theft
July 18, 2002

Mr. Chairman, members of the Committee, I am Boris Melnikoff, a member of the American Bankers Association's Fraud Prevention Oversight Council and Consultant to the Regional President with BB&T in Atlanta, Georgia. I am here on behalf of the American Bankers Association to address industry efforts to protect consumers from the problem of identity theft.

ABA brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Our membership, which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks, makes ABA the largest banking trade association in the country.

Identify theft is on the rise. Stopping ID theft before it occurs and resolving those unfortunate cases that do occur is of utmost importance to the banking industry. Banks have a long and proud history of securing their customers' information. As technology and the Internet have made more information readily available – for better or worse – we have redoubled out efforts to help educate consumers about how to prevent and resolve cases of identity theft. Banks and our customers are partners in protecting information.

The Committee has asked us to outline current efforts on the part of banks to protect customers from identity theft. ABA is pleased to discuss these efforts as the education of consumers and the training of bank employees is crucial in detecting and preventing identity theft.

In my statement, I would like to make three key points:

- The banking industry has been actively involved in the ongoing effort to educate consumers on how best to protect themselves from being victimized by identify thieves. Consumer education begins with the recognition that each of us can limit our vulnerabilities to this crime.

- The American Bankers Association has developed many materials for our member banks – including videos, articles and statement stuffers – to assist in training bank personnel on identity theft prevention and to facilitate outreach programs in banks' communities.

- It is important for the private and public sectors to pursue technological innovations to improve individual identification techniques, beginning, for example, with improved standards for the issuance of drivers' licenses, in order to better combat identify theft at the time the thief seeks to profit from it.

Identity theft harms consumers, financial institutions and severely challenges law enforcement. The efforts mentioned below are only successful if these three groups work in tandem.

What is Identity Theft and What Can We Do to Stop this Crime?

In general terms, identity theft occurs when someone uses another's personal identifying information (name, address, social security number or other related information) to commit any of a wide array of fraud. This ranges from using another's name to obtain a cell phone or apartment lease, to using the information to open credit card accounts, obtain a mortgage, and even commit more heinous crimes such as terrorism.

In specific terms, according to the federal law covering this activity (18 USC § 1028), it is a crime for anyone to:

> Knowingly [transfer] or [use], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

Measuring the scope of identity theft is not an easy task. There have been a number of statements issued by law enforcement, consumer groups and the media attempting to measure the scope of the identity theft problem. For example, Attorney General John Ashcroft has stated that an "estimated 500,000 to 700,000 Americans have their identity stolen" each year. Regardless of the precise number of cases, one thing is clear: identity theft is a major concern to consumers and financial institutions alike, and all of us can do more to address this potentially devastating crime.

In 1997, when changes to Section 1028 were first being debated, the American Bankers Association was very supportive of efforts, led by Senator Kyl, to add additional tools to help bring perpetrators of ID theft to justice. ABA released a strong statement of support on this measure to Senator Kyl, pointing out: "As an industry that works with law enforcement in constantly combating fraud and other criminal acts against financial institutions, we are grateful for your interest in adding prosecutorial tools to this effort."

Unfortunately, even after the changes proposed by Senator Kyl were made to the federal law on identity theft in 1998 – ***which made it easier for law enforcement to bring an action in these cases*** – there was no appreciable increase in prosecutions. We were encouraged, however, by the Justice Department announcement in May that a nationwide effort, led by U.S. Attorneys has resulted in 73 criminal prosecutions for identity theft. Nonetheless, it appears that a primary reason prosecutions have not increased is because losses on typical identity theft cases have fallen below the dollar threshold set by law enforcement that would trigger their active involvement. Our industry remains concerned about those high thresholds that must be reached before an identity theft case is considered for prosecution. Therefore, we believe more needs to be done, and we applaud the Justice Department's recent initiatives in this area.

Banking institutions already dedicate substantial resources towards assisting law enforcement in its efforts, and continue to do more everyday. For example, banks have a new, affirmative duty to

report ID theft under the "Suspicious Activity Report" (SAR) regulations. This requirement (of the Financial Crimes Enforcement Network's (FinCEN)) to specifically file SARs on identity theft provides a vital avenue for reporting this crime.[1] This will not only help facilitate prosecutions, but will also provide better data on the extent and nature of the crime. This, in turn, will help focus the training for bank staff and give the government a better feel for where banks are finding this fraud. With this information, banks now have another means to assist identity theft victims in getting their cases reviewed by law enforcement.

The Banking Industry Has Been Actively Involved in the Ongoing Effort to Educate Consumers

The members of the American Bankers Association have been leaders in the private sector's push to educate consumers about how they can protect themselves. Central to prevention is the recognition that each of us can limit our vulnerabilities to this crime. We realize that people need our expertise and guidance to avoid being victimized. As several government agencies, such as the Federal Trade Commission, the United States Secret Service and the Postal Service have done, the banking industry has offered a number of tips to consumers on protecting one's personal information.

For example, on the following page, I have included many common sense precautions we can all take. This listing was written by Lynne Sanders of JP Morgan Chase & Co. for the May/June issue of ***ABA Bank Compliance Magazine.***

1 As the Treasury bureau charged with handling these reports, FinCEN has indicated: Criminal activity related to identity theft or pretext calling has historically manifested itself as credit or debit card fraud, loan or mortgage fraud, or false statements to the institution, among other things. As a means of better identifying and tracking known or suspected criminal violations related to identity theft and pretext calling, a banking organization should, in addition to reporting the underlying fraud (such as credit card or loan fraud) on a SAR, also indicate within the narrative of the SAR that such a known or suspected violation is the result of identity theft or pretext calling. Specifically, when identity theft or pretext calling is believed to be the underlying cause of the known or suspected criminal activity, the reporting institution should, consistent with the existing SAR instructions, complete a SAR, " See Special SAR Form Completion Guidance Related to Identity Theft and Pretext Calling, SAR Activity Review June 2001, pg. 37.

Precautionary Measures to Stop ID Theft[2]

The following list provides tips on how you — and your bank customers — can stop an ID theft before it happens. Proactive measures provide the best protection for your assets and your good name.

1. Do not give out financial information such as checking account and credit card numbers — and especially your Social Security Number — on the phone unless you initiate the call and know the person or organization you're dealing with.
2. Do not pre-print your driver's license, telephone, or Social Security numbers on your checks.
3. Report lost or stolen checks immediately. Also, review new checks to make sure none has been stolen in transit.
4. Store cancelled checks — and new checks — in a safe place.
5. Guard your personal identification numbers (PINs) for your ATM and credit cards, and do not write on or keep your PINs with your cards. You should also guard your ATM and credit card receipts. Thieves can use them to access your accounts.
6. Be creative in selecting personal identification numbers for your ATM and credit cards, and passwords that enable you to access other accounts. Do not use birth dates, part of your Social Security Number or driver's license number, address, or children's or spouse's names. Remember: If someone has stolen your identity, he or she probably has some or all of this information.
7. If you receive financial solicitations that you're not interested in, tear them up before throwing them away, so thieves can't use them to assume your identity. Shred or make unreadable any other financial documents, such as bank statements or invoices, before disposing of them.
8. Do not put outgoing mail in or on your mailbox. Drop it into a secure, official Postal Service collection box. Thieves may use your mail to steal your identity.
9. If regular bills fail to reach you, call the company to find out why. Someone may have filed a false change-of-address notice to divert your information to his or her address.
10. If your bills include suspicious items, do not ignore them. Instead, investigate immediately to head off any possible fraud before it occurs.
11. Periodically contact the major credit reporting companies to review your file and make certain the information is correct.

For a small fee, you can obtain a copy of your credit report at any time. (Please note that in some states or municipalities, you may be legally entitled to these reports free of charge. Check with the credit bureau when ordering the report.) The three major credit bureaus and their phone numbers follow:

Equifax	(800) 685-1111
Experian	(800) 682-7654
TransUnion	(800) 916-8800

[2] See Lynne Sanders, "Stopping ID Theft in It's Tracks," ABA Bank Compliance, May/June 2001, pgs. 35-39.

ABA members have worked diligently to see to it that these types of "ID Theft Primers" are communicated frequently to both customers directly and to bank employees for outreach to the community. One of the best resources to combat identity theft is self-awareness of how you can protect yourself. We believe that taking many of these small steps, while not eliminating identity theft, will diminish the frequency of this crime.

The American Bankers Association Has Developed Many Materials for Our Member Banks

Mr. Chairman, and members of the committee, with my long history in corporate security, I am very pleased to report that the banking industry and our leading trade group, the American Bankers Association, have been tremendous examples of how to increase awareness of this invidious crime.

- In 2000, the American Bankers Association distributed to *all* of its members an "ID Theft Communications Kit." This kit, available on the ABA's website, was designed to help bank employees deliver the message of ID Theft prevention to consumers throughout the country. The kit contains public service announcements, sample statement stuffers and a sample newspaper column that a bank official could tailor to his or her community. We have provided a copy of this kit to the Committee.

- In the same year, ABA distributed a Video News Release (VNR) to promote public awareness of identity theft that reached an estimated 28.6 million viewers. To reach radio listeners with the same message, ABA staff and bank officials presented prevention tips to an estimated 10.8 million listeners. For the print media, ABA distributed a column that generated 1,008 newspaper articles with a readership estimated to be nearly 41 million.

- On a continual basis, ABA offers separate statement stuffers for banks to use in mailings to consumers, with close to six million distributed across the country.

Moreover, the Association makes sure that its various banker-training programs include sessions on identity theft. For example, at the 2001 ABA Regulatory Compliance Conference, a three-hour session was held for compliance officers, attorneys and auditors on privacy, identity theft and information security. We duplicated that effort in June of this year at the 2002 event. Another training delivery mechanism, the phone briefing, has also been used to communicate the message on prevention. ABA has been fortunate to have representatives from the Secret Service and the nationally known identity theft trainer, Robert Douglas (President of American Privacy Consultants), to assist in these efforts. ABA has also sponsored Mr. Douglas to provide identity theft and pretext calling prevention-training seminars. I have attached an article that highlights the benefits of these seminars.

- The ABA has also created a web page devoted completely to fraud solutions, including a page with consumer tips on identity theft prevention/solutions, and has endorsed the FTC's "KnowFraud" education campaign. The website also provides important links to various agency websites that cover this type of fraud.

- Finally, the Association was able to take advantage of an excellent training video on pretext calling and identity theft produced by JP Morgan Chase & Co. ABA has repackaged that tape for broad distribution to our membership. To date, we have sent out over 1,200 of these tapes and continue to provide the product free of charge to ABA members. A copy of this tape has also been supplied to the Committee.

While the ABA has done considerable work in this area, we realize that individual industry efforts must continue. Fortunately, many of our members are engaged in similar efforts around the country. I continue to witness superb examples of industry outreach, a few of which I want to share with the committee:

- ***Bank of America and the National Consumers League***

  Bank of America has recently announced a customer protection campaign, created in partnership with the National Consumers League to help educate consumers about identity theft. The project, called the "Invasion of the ID Snatchers," includes public service

announcements, a web site with tips for avoiding identity theft, and a variety of other materials consumers can use to protect their privacy on the Internet and elsewhere.

The new web site includes tips for consumers on preventing and recovering from identity theft, as well as a very useful overview of common scenarios explaining how thieves steal personal information and what they are able to do with it.

In addition, Bank of America has also issued press releases on some broad-based e-mail scams. Media coverage resulting from the press releases have added value as they reach beyond the individual institution's customers to the public at large. ABA also urges the government to continue to issue fraud warnings through press releases and other communications to notify trade groups.

- ***California Bankers Association and Elder Abuse Prevention***

  A member of ABA's Compliance Executive Committee is chairing the California Bankers Association's task force on financial elder abuse prevention. They are working with a consortium that is producing an educational videotape for banks, as well as model procedures and policies. Similar efforts are underway in other states and localities.

- ***Commerce Bank and Trust (Topeka, Kansas)***

  Bank officials from Commerce Bank and Trust have given presentations to senior groups, including the Topeka Chapter of the AARP, on the various ways people can protect their personal information. In addition, the bank explains the process for credit reputation restoration and how to minimize fraud losses. This is just one example of hundreds of similar events occurring throughout the country.

- ***JP Morgan Chase & Co.***

  Several other large institutions have made identity theft outreach a major priority. In the previously mentioned ABA Bank Compliance article, JP Morgan Chase & Co. emphasized its education of both employees and the public. In 2000, JP Morgan Chase launched a nationwide awareness campaign that included both proactive and reactive measures. Two events are particularly important to cite. Programs were held in Houston and New York that

focused on elderly and minority members of those communities and the need to increase awareness of identity theft. Other participants included the U.S. Postal Inspectors Officer, the FTC, and AARP.

- *Comerica*

  Comerica, based in Detroit, hosted an "Identity Protection Week" and developed a "Victim's Recovery Kit" which includes sample letters to credit bureaus and financial institutions, as well as a log for recording actions taken to report the crime. This type of assistance especially helps those who are unsure of how to manage the information minefields that accompany this fraud.

Improvement Needed for Issuance of Identification

Mr. Chairman, while there remains some debate on what other options exist to improve the ability of banks and consumers to protect consumers against ID theft and punish those that commit this crime[3], ABA urges consideration of new government leadership directed toward improving identifications. Specifically, the Congress should direct its attention to the nascent move to improve the current system of how states issue drivers licenses. There is no better way to protect against fraud and terrorism then by improving the identification documents used to complete financial and other business transactions. The American Association of Motor Vehicle Administrators (AAMVA) has offered an excellent outline of how to proceed. AAMVA has urged Congress, and ABA concurs, that there needs to be "minimum compliance standards and requirements that each state must adopt when issuing a license." We urge Congress to schedule additional hearings on this important topic as soon as possible.

Thank you for the opportunity to update the committee on our industry's efforts in the important area of educating the public on the identity theft issue.

[3] The Attorney General and the Chairman of the Federal Trade Commission have endorsed another proposal (S. 2541) that enhances the Federal law covering identity theft. The measure, among other things, creates a new crime of aggravated identity theft. If this change can help prosecutors take cases the industry certainly supports that goal.

ABA Bankers News
July 9, 2002
The Biweekly Newspaper of the American Bankers Association Volume 10, Issue 14

Article Reprint

Identity Theft Prevention Workshops

By Patrick Dalton

Because of the nationwide increase in identity theft and bank fraud, ABA has contracted with highly respected security expert Rob Douglas, CEO of American Privacy Consultants Inc., Oak Creek, Colo., to provide identity theft prevention workshops for banks. Tom Scalavino, group vice president/compliance officer at Compass Bank in New Bedford, Mass., recently hired Douglas to conduct a workshop for employees at his institution. ABA Bankers News asked Scalavino to talk about the workshop and some of the things the employees learned.

Scalavino

I truly believe that anyone who invites Rob Douglas to their bank to enhance identity theft training and pretext calling training will benefit immensely. I strongly recommend him.

Q. How did you hear about Rob?

A. I had read various articles quoting Rob on pretext calling. Subsequently, I met him at the ABA Compliance Conference in Washington, D.C., last year. That's how it all started. Pretext calling was one of the issues we were very concerned about. We felt his booklet from ABA on pretext calling ("Privacy and Information Security — An Awareness Guide") was very good, and we made it the basis for our initial in-house training. We also addressed various privacy issues with him. He was very knowledgeable. We asked Rob for his assistance on conducting pretext calling tests within the bank. Based on his experience and background, we felt Rob would certainly be of great assistance to us in pretext calling training and identity theft prevention training.

Q. How did the workshop work?

A. We invited Rob to New Bedford to conduct two three-hour sessions — one on April 10 and another on April 11. We encouraged individuals from every functional area of the bank — loan officers, loan processors, assistant branch managers and branch managers etc. to attend. The training was primarily for employees and officers whom we felt were in the front line of receiving calls that might compromise customer information security, if one was not properly trained nor sufficiently vigilant. Between the two sessions, about 140 employees attended.

Q. What are some of the things that jumped out at the employees?

A. I think they were alarmed as to how easy it is for someone to initiate pretext calls and impersonate someone else. They learned how certain individuals access the Internet to make false IDs. The ease of buying and sharing information on the Internet was very scary and quite enlightening to all of our employees. Rob demonstrated how information brokers pretend to be somebody else, such as claiming they work for an insurance company. They attempt to obtain some information from one employee, and then they call back and get more information from someone else. That was very informative to our personnel.

Rob also discussed several information broker stings he has been involved in. He showed a videotape spotlighting an information broker bragging on how easy it was to get information. The employees heard that, and I think it placed them on guard quite a bit more.

See Identity Theft/P

Identity Theft Prevention

From page 1

Q. What impressed you personally?

A. I had heard Rob speak at the ABA Compliance Conference, but actually seeing how the information is so easily and readily available for anyone who wants to impersonate someone else really got my attention. These people have no conscience. They are just out for the money, and they sell the information.

Rob went over the case of Amy Boyer, the Nashua, N.H., girl who was killed by a stalker after he paid about $220 to an Internet information broker to obtain the address where she worked. Amy's story really stood out and had a tremendous impact on everyone.

Q. Does the identity theft training have any implications for the terrorism issue?

A. Yes. The ease with which these individuals can create various identities and impersonate people has a tremendous impact on terrorism. It emphasizes how careful we must be in complying with established account-opening procedures to ensure that we identify the party in front of us. We must be very alert during every transaction, and be sure to know your customer. It is not simply obtaining an ID and quickly writing some information down by rote. It's making sure the description on the ID matches the individual in front of you. That's another important reminder folks walked away with — to be much more attentive during account-openings.

Q. What kind of reviews did Rob's presentation get from the employees?

A. I have 40 or 50 evaluations, and they are all along the same lines: "Excellent meeting." "Great information on a very serious subject." "I thought the presentation was very informative, and Rob is a fantastic instructor." Numerous employees thought the information also helped them personally — specifically, to be somewhat more cautious and a bit more protective of themselves, and to be more aware of their own accounts, their own surroundings and how they discard their personal mail.

Q. Would you recommend Rob's workshop to other bankers?

A. I truly believe that anyone who invites Rob Douglas to their bank to enhance identity theft training and pretext calling training will benefit immensely. I strongly recommend him.

For more information on the identity theft prevention workshops, go to www.privacytoday.com or call Rob Douglas at 970-736-1060.◆

Senator CRAIG. With the indulgence of the panel and the audience, there is a vote underway and my primary responsibility being in this body is to vote. So we will stand in recess for a few moments while I run and vote and I will return as quickly as I can to proceed with the balance of the panel and questioning.

The committee will stand in recess. [Recess.]

If I could ask everyone to take their seats and for the panel to reassemble, please.

Boris, we just finished with you, and let me tell you that the effort that it appears the American Bankers Association has underway with both public outreach, but also education of professional staff of employees sounds impressive and is important and I am glad to hear that.

Now, let me turn to Stuart Pratt, Executive Director, Consumer Data Industry Association here in Washington. Stuart, welcome before the committee.

STATEMENT OF STUART K. PRATT, VICE PRESIDENT, GOVERNMENT RELATIONS, CONSUMER DATA INDUSTRY ASSOCIATION, WASHINGTON, DC

Mr. PRATT. Mr. Chairman, thank you for inviting us here today, and for the record, I am Stuart Pratt, Vice President, Government Relations, for the Consumer Data Industry Association.

Senator CRAIG. That is a much more impressive title than I gave you.

Mr. PRATT. But I appreciate the promotion, actually.

Senator CRAIG. All right. Thank you. [Laughter.]

Mr. PRATT. We are the association which represents all of the nation's largest credit reporting systems, check approval systems, and mortgage reporting systems, and so, obviously, we play a very central role in these types of debates.

In fact, we applaud you for holding this hearing because identity theft is a pernicious crime. It is a difficult crime for everyone involved. We all end up, as a result of the criminals' activities, trying to untangle this snarl of accounts and information, and sometimes it goes smoothly and sometimes it goes very well, and then sometimes you have seen cases where it does not go as smoothly as we would like for it to go.

We thought we would focus on just two messages today in terms of, first of all, what have we been doing as an industry to try and work through and actually alter practices, business practices, that will make it easier for victims to keep their information safe and sound and to bring their credit history back to whole, and also, we wanted to focus, as well, on consumer education and how educational efforts, we think, do play an extraordinarily important role.

We looked at this issue as far back as 1997, and by March of 2000, we had issued a six-point program that would assist victims. The six-point program is outlined in a press release which is attached to the testimony today. Let me just highlight a couple of key steps that we thought were particularly important in this six-point program.

First, we standardized the security alert. When you contact the credit bureau, one of the first steps we will take is to put a security

alert on your file. It is a text message and it says, "I have been a victim of identity theft. Please do not grant credit. For example, here are telephone numbers you can use to verify who I am." Obviously, if you have a telephone number and you are standing in front of the consumer, unless you have a cell phone strapped to your hip, there should be some interplay there that allows a lender to be able to make a better risk decision about who they are doing business with.

By standardizing the alerts, both in terms of the text itself and also by adding an alphanumeric sequence, which is a fancy way of saying a code, at the beginning of the security alert, we think this better enables every one of our lender customers to be able to look for that alert message, to look for the code, and to take the actions that they think are appropriate based on that information.

So that obviously gives us a way of, downstream, trying to help the consumer stay whole, because that alert message remains on the file and it is a decision that we make jointly with the consumer during the consumer relations process.

We also know that consumers like standardization across the spectrum, so there are three major credit reporting systems in this country and most consumers we interviewed, by the way, in our process, said, we would like to have the same kind of treatment each time so we do not have to go through three different versions of the treatment.

In this case, what we did is we said, we will do three things first for the consumer. When you contact us, even if you are just leaving a message on an automated voice attendant, we are going to put a security alert on your file. We are going to take you off of any direct mail offers of credit, opt you out of any non-initiated transaction, so only when you go and apply for credit will your credit report be used. Third, we will get your report to you in the mail within three business days, often quite a bit sooner than that, and obviously, there are Internet deliverables, as well, today. But those three steps ensure the consumer has a better continuity across the three credit reporting systems.

Then we also designed a system on the back end which is our attempt to be responsive to the fact that identity theft is more longitudinal than some other types of crime. It is more difficult for us to know, is it over? Am I finished? Or do I still have a problem that is latent, that is out there? Is there more credit that I just am not aware of yet that was not yet reported to the credit bureau, for example?

So over the course of the next 90 days, once we have brought a file back to current, we will then send the consumer additional copies of his or her file with the 800 number, with access to live personnel. It keeps the consumer engaged—and this would be true for a senior or for any other consumer who is a victim—keeps them engaged. Look at your file. Tell us if there is something else wrong with that file so we can take care of that.

Now, we also knew that consumers wanted escalated services. We want to be believed. That is one of the key points that many consumers have said. How hard is it to prove who I am? So we agree with all the testimony that has said, get a police report. If you get a police report, we will immediately with that police report

block the fraudulent information. We will not wait to check with the lender. We will take your word for it. The police report is a validating document for us. We will block the fraudulent data. This should give a consumer a chance to get on with their life much more quickly and to be able to bring their credit report whole much more quickly, as well.

Finally, we do accept the FTC's standardized fraud affidavit, which again reduces the paperwork burden, if you will, for victims, and that is another key component of this. How many different affidavits do I complete? How much money do I have to pay to have them notarized, and so on and so forth.

We think consumer education is another key component of this, and I know a lot of times we talk about consumer education as a replacement for other actions. But as you can see, we have taken procedural actions with our business model to change what we do for victims. But consumer education clearly allows us, for example, to be able to partner up, and in our case, we committed ourselves to partnering up with a group called Call for Action. We did produce a brochure, and this brochure is maybe in some ways a simplified version of the type of information that the Federal Trade Commission promulgates. We, in fact, encourage consumers to contact the FTC.

We also promulgate information on victims' rights under the law and encourage consumers to understand their rights under the law. For every citizen, by the way, the Fair Credit Reporting Act is not obvious, and so we produce a flow chart that says very simply, this is what should happen when you contact the credit bureau, dispute your information, and get that information corrected.

We have seen more data, and we have indicated this in our testimony, where data shows that we are making progress. More consumers are calling our fraud units, taking a preventative step, so maybe that is the last, most important point I can leave with you. As opposed to calling and saying, "I am a victim," the majority are calling and saying, "I want to take a preventative step to make sure I do not become a victim." That is good news in terms of the consumer education.

Let me close with that. I see my time has expired and I am open for questions and I thank you for the time that you have.

Senator CRAIG. Stuart, thank you for that testimony.

[The prepared statement of Mr. Pratt follows:]

STATEMENT OF

STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION
WASHINGTON, D.C.

BEFORE THE

Special Committee on Aging

United States Senate

ON

Identity Theft

July 18, 2002

Mr. Chairman, and members of the Committee, thank you for this opportunity to appear before the Senate Special Committee on Aging. For the record, I am Stuart Pratt, vice president, government relations for the Consumer Data Industry Association.

CDIA, as we are commonly known, is an international trade association representing approximately 500 consumer information companies that provide credit and mortgage reporting services, fraud prevention and risk management technologies, tenant and employment screening services, check fraud prevention and verification products, and collection services, as well.

We commend you for holding this hearing on the crime of identity fraud. It is an equal-opportunity crime that can affect any of us. Identity fraud is a particularly invasive form of fraud where consumers, consumer reporting agencies and creditors must untangle the snarl of fraudulent accounts and information resulting from a criminal's actions. The task can be frustrating, and, in severe cases, time-consuming for all concerned.

The Committee has asked us to outline our members' efforts to protect consumers from identity fraud. In that regard, let me focus on two points today:

- CDIA members have been at the forefront of efforts to understand the nature of this crime for years and they have established victim assistance procedures, which go beyond the requirements of any law.

- Consumer education is a mainstay of any successful campaign to reduce the incidence of identity fraud. Though preliminary, some data indicate that industry and governmental efforts to reach consumers is working.

CDIA Voluntary Victim Assistance Programs:

In March of 2000, the CDIA issued a news release (included with this testimony) which outlined the credit reporting industry's six-point victim assistance program. Ours was the first industry to step forward and not merely educate its members about the problems consumers experienced, but to seek specific changes in business practices. These ID fraud victim assistance initiatives were the culmination of internal reviews of current processes by senior fraud personnel; interviews with law enforcement, victims and privacy advocates; as well as input from our association's outside counsel to this effort, former Vermont Attorney General, M. Jerome Diamond. The industry's voluntary initiatives became effective on January 1, 2001, and while our attached news release outlines all six initiatives, let me highlight a few for the Committee.

Standardizing Security Alerts – Prior to the CDIA's initiative, the three credit reporting systems were already voluntarily administering a system of security alerts, which are text messages (often accompanied by a code) included in a consumer's credit report, which notify lenders and other users of the report of the fact that a consumer has contacted the credit reporting system and believes that he or she is a victim of identity fraud. The alerts contain, at the consumer's request, one or two telephone numbers for the lender to use in contacting the consumer to verify that he or she is truly seeking a new line of credit or other service.

The CDIA's initiative sought to improve the effectiveness of these alerts in two important ways:

- The text of the security alerts is now standardized with the goal of ensuring that the consumer's request is honored regardless of which credit reporting system is used by a lender.
- The text message is now preceded by an alpha-numeric code that ensures that even in a computer-to-computer transmission, the fact that a security alert is part of a consumer's file is easily identified by the lender's system.

The security alert is transferred with any consumer credit report, whether it is a highly codified version, or summarized or otherwise formatted for a particular lender's system.

Standardizing the First Three Steps – In our interviews with consumer victims, we learned that consistency of experience is important. When consumers learn that they are victims of identity fraud, they are often advised to order a copy of their file disclosure (i.e., credit report) from each of the three credit reporting systems. Under the CDIA initiative, when consumers call any one of the automated systems to order their file disclosures, they can now have confidence that the same three key steps will be taken:

- A security alert will be added to the consumer's file ensuring that if a criminal is still active, that subsequent lenders will know that the consumer may be a victim of identity fraud.

- The consumer's file will be opted-out of any direct-mail offers of credit or insurance, thus ensuring that only where the consumer initiates a transaction will the consumer's file be accessed.
- The consumer's file will be placed in the mail to the consumer within three business days or the consumer's request.

Following Up – Consumers victims expressed frustration with the difficulty of knowing whether or not the crime was "over." In an effort to help consumer victims stay actively involved with our members where ID fraud has occurred, CDIA's credit reporting members altered their practices. Specifically, after a consumer's file has been corrected and the fraudulent data has been removed through a traditional reinvestigation process, our members will then continue to send the ID fraud victim additional copies of his or her file during the next 90 days. With each file, the consumer will have a toll-free number, which provides access to live personnel and thus, if the consumer spots additional problems with the file, he or she can contact our members quickly and have the problem resolved. This 90-day service extends beyond the requirements of the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 *et seq.*) and helps mitigate the effects of this longitudinal crime.

New Victim Assistance Procedures and Police Reports – Victims of identity fraud want to be believed when they claim that they are victims of the crime, and they want their situation addressed quickly. Our members looked for a safe and sound process to meet this need and as you can see in our attached letter to the Federal Trade Commission, our members have not only committed themselves to removing fraudulent data upon request of a victim who has a police report, but we have coordinated this effort with the FTC's ID Theft Clearinghouse. Following are

the comments of J. Howard Beales, III, Director of the FTC's Bureau of Consumer Protection, regarding our members' program.

> "Another collaborative effort with tremendous promise is your new police report initiative. Through this program, the three agencies have agreed to block any credit line when they receive from the consumer a copy of the police report documenting the identity theft. And, last year the IACP passed a resolution encouraging local law enforcement to issue police reports to ID theft victims.[1] We're doing our part too, developing a training video with IACP to encourage the police to issue the reports. I appreciate that certain consumer-based initiatives require you to balance accuracy issues – knowing that the consumer's report contains all relevant credit information, including derogatory reports – against customer service. From my perspective, your police report initiative strikes just the right balance. You have an assurance of the consumer's good faith, evidenced through the official police report, and the consumer will be untouched by the false negative information. I encourage the ACB and its members to continue developing programs and systems that ease the burden on identity theft victims."[2]

Acceptance of the FTC Fraud Affidavit – The FTC undertook a complex and laudable task of trying to simplify an ID fraud victim's paperwork burden by creating a single affidavit for multiple uses. A number of our members participated in the work group discussions which lead to the creation of this new form and all of the CDIA's nationwide credit reporting system members accept this affidavit.

CDIA and Consumer Education

Any time a crime is identified, we all want to find the one "silver bullet" which will stop it in its tracks. In reality, layers of efforts and, in some cases, years of work are necessary to truly reduce the incidents of a particular type of crime. In our visits with law enforcement and with consumer groups, it was evident to the members of the CDIA that procedural changes are important, but that consumer education, focused on prevention and post-victim assistance, was essential.

---

1 International Association of Chiefs of Police, *Curbing Identity Theft*, (Nov. 15, 2000) available at http://www.theiacp.org/leg_policy/Resolutions/resolutions2000.htm#idtheft

A Commitment to Call for Action - The CDIA committed financial resources and technical expertise to support the efforts of Call for Action, a consumer educational organization, which is reaching out aggressively to consumers and ID fraud victims. Enclosed with this testimony is a practical, easily understood brochure developed by Call for Action with the assistance of the CDIA. The brochure has been distributed to:

- National and state law enforcement agencies.
- States attorneys general and consumer protection offices.
- Military barracks and educational institutions.
- Call for Action regional affiliate offices.
- CDIA members.

Call for Action reports that more than 200,000 ID fraud brochures have been distributed and another 100,000 are going to print. Further, the information in the brochure is also available on their website and Call for Action reports that they have had more than 125,0000 visitors view their ID fraud information. The brochure, produced by Call for Action, is available at: www.callforaction.org/idtheftintro.html.

Call for Action's efforts also include the production of a video news release (VNR). Their VNR reached 6.7 million viewers nationwide. The VNR included interviews with the FTC and, again, highlighted a message of steps for prevention and for post-victim assistance.

Making sure victims understand their rights – In addition to the many voluntary steps members of the CDIA have taken on behalf of consumer victims, our members must also comply

[2] Excerpt from a speech delivered to the members of the Consumer Data Industry Association by FTC Director Beales on January 17, 2002.

with specific duties under the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 *et seq.*). As important as it is for our members to comply with the law, it is equally important that victims of identity fraud are fully aware of their rights. To help accomplish this goal, the CDIA produced a brochure entitled "The Credit Reporting Dispute Resolution Process." A simple flow chart, which is color coded, ensures consumers understand what must be done with their dispute of fraudulent information each step of the way. It has been an effective educational tool and it won the National Association of Consumer Agency Administrators' Print Media – Private Sector Category Award in 2000. Each year the CDIA sends letters to state consumer protection and states attorneys general offices offering free bulk supplies of this brochure.

Are the efforts of government and the private sector paying off? - There are some trends which are encouraging and which show that our nation is making progress on this issue. The efforts of the FTC, our industry and others to educate consumers about the crime of identity fraud appear to be making headway.

First, our own members report that the majority of consumers who contact our credit reporting members' fraud units are taking preventative steps and are not reporting an actual crime. This is a strong indicator that the message is getting out to consumers to exercise caution and quickly take the right actions to protect themselves.

Regarding victims of the crime, the FTC's own ID fraud trend data shows that 42[3] percent of the consumers who contacted the FTC learned about the occurrence of the crime in less than a

[3] Federal Trade Commission Report produced by the Identity Theft Clearinghouse entitled "Identity Theft Complaint Data, *Figures and Trends on Identity Theft*", November 1999 through June 2001, Page 4.

month. This percentage is fully ten percentage points higher than the statistic cited in the FTC's previous report. Here too, we see that where consumers are educated, they are learning how to spot the crime and take steps to limit the extent of the criminal's activity. Ultimately consumer education remains one of the best crime-prevention efforts on which we can continue to focus.

Summary

In conclusion, we believe that since this crime began being debated publicly, a great deal has changed. Our members have voluntarily adjusted their practices to better assist victims. The educational efforts of the private sector and the efforts of government are making progress with consumers, both in terms of a improving a consumer's understanding of prevention and post-victim assistance steps that can be taken. New laws have been enacted to define this crime and to clarify that consumers are clear victims. This point may seem to be less significant today, at one time victims' top complaint was merely that law enforcement didn't consider them to be victims under a crime statute. We continue to applaud the enactment of the "Identity Theft and Assumption Deterrence Act of 1998" (Pub.L. 105-318) and the more than 30 state laws which our members have actively supported.

In all of this, while procedures will help victims and reduce application fraud, and while consumer educational efforts will continue, we believe that it is critical is that Congress ensure that law enforcement has the resources necessary to enforce the law. Ultimately, identity fraud isn't a consumer protection issue begging for new laws. It is a crime prevention issue in need of large-scale, coordinated efforts to investigate and prosecute criminals. Law enforcement needs the financial support of Congress to get the job done. Everyone who even considers perpetrating

identity fraud, should also know that they will be pursued, prosecuted and incarcerated. These criminals deserve nothing less.

Thank you for this opportunity to appear before this Committee and to share our views. I am happy to answer any questions you may have.

Associated Credit Bureaus, Inc.
1090 Vermont Ave., N.W.
Suite 200
Washington, D.C. 20005-4905
Tel. 202.371.0910
www.acb-credit.com

November 16, 2001

Ms. Betsy Broder
Assistant Director
Division of Planning and Information
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

RE: Assisting Identity Fraud Victims – New Police Report Initiative

Dear Betsy:

Early this year ACB briefed you and your staff on a new consumer reporting industry voluntary initiative, which was still being implemented on a nationwide basis. This initiative involves using police reports as a validating document for consumers who claim they are victims of the crime of identity fraud. The police report initiative is now fully implemented, and we hope that FTC consumer assistance advisors will apprise identity fraud victims who contact the FTC hotlines of this new credit reporting industry procedure.

More specifically, this initiative involves the major credit reporting systems within our membership, and the actions they will take on behalf of consumers when their dispute of fraudulent information is accompanied by a police report. When a police report is provided as part of the process of disputing fraudulent data, Equifax, Experian and TransUnion will block these disputed items from appearing on subsequent consumer reports regarding that individual.

Our initiative is a recognition that identity fraud victims want to solve the problems resulting from the crime as quickly as possible. By accepting a police report as a validating document of a consumer's circumstance and blocking data prior to a reinvestigation, our members are greatly improving a victim's circumstances by facilitating faster resolution. While our police report initiative is resistant to fraudulent credit repair schemes, which often result in disputes of accurate information in credit files, it is not immune[1] and we urge the FTC to continue its excellent work in enforcing the Credit Repair Organizations Act (15 U.S.C. 1679 *et seq.*).

[1] Our members have received police reports which appear to be fraudulent. Even the most well-intentioned voluntary initiatives of industry seem to be immediately taken as opportunities by fraudulent credit repair schemes to attempt to delete accurate, derogatory information.

Ms. Betsy Broder
Page Two
November 16, 2001

Along with specific industry efforts such as this police report initiative or the six-point program announced March 14, 2000, ACB has also been focused on consumer and industry education with regard to the crime. Attached is a brochure which ACB helped design and fund through Call for Action, a nationwide network of consumer hotlines. You will see in the body of the brochure that among other advice, we urge consumers to report their experience to the FTC's response center. To date, more than 100,000 copies this brochure has been distributed to organizations and consumers, and plans for an additional 100,000 brochures are in the works.

We have also included a copy of a brochure which was developed by ACB and which consumers value greatly because it lays out the consumer relations process of the credit bureaus in a flow chart format. ACB distributes thousands of these brochures each year to state attorneys general, state consumer protection offices, state insurance commissioners and more.

The FTC has, of course, played a leading role in educating and assisting consumers regarding identity fraud. We applaud your efforts. In fact, during the past twelve months we have promoted ACB member awareness of the FTC's toll free number for victims and your extensive web site resources in our association publication, COMMUNICATOR, which reaches 1300 executives each month. In promoting the FTC's Sentinel system, we hope that the database of self-reported cases of identity fraud will become an essential investigative tool for law enforcement. We continue to believe that law enforcement efforts are a critical component in addressing the crime of identity fraud. Without an effective record of prosecutions, criminals will continue to believe that there little consequence for this crime, it will continue unchecked

In closing, we hope you find the information we've provided useful. Please give me a call if you have any questions (202.408.7416).

Sincerely,

Stuart K. Pratt
Vice President
Government Relations

Cc: The Honorable Timothy J. Muris
Howard Beales, Director, Bureau of Consumer Protection
Joel Winston, Acting Director, Financial Practices Division
Hugh Stevenson, Director, Division of Planning and Information

Associated Credit Bureaus, Inc.
1090 Vermont Avenue, N.W. Suite 200
Washington, D.C. 20005-4905

NEWS RELEASE

Contact: Norm Magnuson
Vice President of Public Affairs
202/408-7406

For Immediate Release
March 2000

Credit Reporting Industry Announces Identity Theft Initiatives

Associated Credit Bureaus, the international trade association for the consumer reporting industry, announced today a commitment on behalf of the nation's leading credit reporting agencies, to voluntarily implement a comprehensive series of initiatives to assist victims of identity theft in a more timely and effective manner.

"While there is no evidence to show that the credit report is a source for identity theft, our industry has always taken an active role in assisting consumers who are fraud victims. Our members have taken this responsibility seriously, and we're very proud of these initiatives that help consumers who are victims of identity theft or fraud," noted D. Barry Connelly, president of Associated Credit Bureaus. "Designing and implementing these initiatives is a significant milestone in the ongoing efforts of our industry to help address the problem of identity theft. As long as there are criminals who prey on innocent consumers, we will continue to seek even better ways to serve consumers and work with law enforcement and our industry's customers to address this threat."

Connelly outlined the industry's six-point program to improve identity theft victim assistance:

· Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.

· Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.

· Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.

· Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.

· Launch new software systems that will monitor the victim's corrected file for three months, notify the consumer of any activity, and provide fraud unit contact information.

· Fund, through ACB, the development of a series of consumer education initiatives through ACB to help consumers understand how to prevent identity theft and also what steps to take if they are victims.

ACB's initiatives, to be fully implemented within seven months of this announcement, resulted from a task force comprising senior executives from the ACB Board of Directors and former state Attorney General, M. Jerome Diamond. Diamond interviewed consumer victims and law enforcement officials, made on-site visits to credit reporting agency fraud units, and obtained input from privacy advocates. His counsel was an integral part of the decision-making process and influenced the final content of the initiatives.

Connelly said: "Identity theft is a crime that is deeply unsettling for the victims. Our initiatives will make it easier for victims to put their financial lives back together." Connelly stressed, though, that the crime extends beyond individuals to creditors and ACB members, and added, "We must all work together in the areas of prevention and victim assistance. We supported the enactment of the Identity Theft Assumption and Deterrence Act of 1998 and have worked with more than half of the state legislatures on similar laws. We urge law enforcement to vigorously investigate and prosecute the criminals."

Associated Credit Bureaus, Inc. is an international trade association representing 500 consumer information companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services and collection services.
Source: Associated Credit Bureaus, Inc.
Web site: www.acb-credit.com

# # #

Stuart K. Pratt
Vice President Government Relations
Associated Credit Bureaus, Inc.
Washington, D.C.
202.408.7416 - Direct

identity **theft**

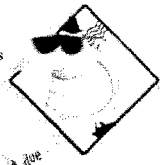
your good name gone bad

what **is identity theft**?

Identity theft is when someone obtains a person's identifying information, such as name, address, date of birth, social security number or mother's maiden name. Using this information illegally, an imposter can open new credit card accounts, drain your bank accounts, purchase automobiles, apply for loans, open utility services and on and on.

No matter how cautious you are, you cannot guarantee that a criminal will not obtain your information. The following steps will tell you what the warning signs are, how to protect yourself, what to do if you become a victim and the resources you will need.

warning signs



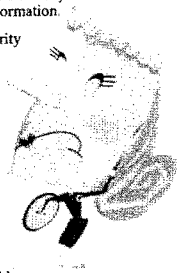
Often, there are no warning signs that identity theft has occurred. However, some reasons for concern are:

- Your monthly credit card and bank statements suddenly stop arriving.
- You are denied credit for no apparent reason.
- You start getting bills from companies you do not recognize.
- Credit collection agencies try to collect on debts that do not belong to you.

how to **protect** yourself!

Personal Information

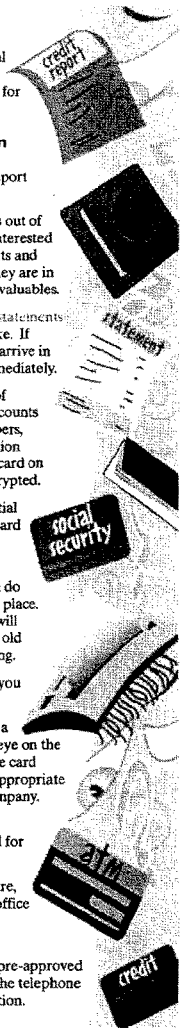
- Ask your bank, doctor's office, other businesses and your employer how they use and protect your personal information.
- Never carry your Social Security card, Social Security number, birth certificate or passport, unless necessary.
- Do not put your address, telephone number or driver's license number on a credit card sales receipt.
- Social Security numbers or phone numbers should not be put on checks.
- Identifying information should not be given over the phone or the Internet to someone you do not know or on a cellular or cordless phone.
- Shred all personal documents before placing them in the trash.



- If your state uses your Social Security number as your driver's license number, ask for another number.

Financial Information

- Get a copy of your credit report every year.
- Keep your financial records out of sight. Burglars are just as interested in credit cards, bank accounts and investment statements as they are in your TV, jewelry and other valuables.
- Check monthly credit card statements for charges you did not make. If monthly statements do not arrive in the mail, call the lender immediately.
- Keep a list, in a safe place, of all credit cards and bank accounts including the account numbers, phone numbers and expiration dates. Only use your credit card on the Internet if it will be encrypted.
- Shred financial or confidential information such as credit card pre-approvals, credit card receipts, etc.
- If you have credit cards you do not use, store them in a safe place. Cancel the accounts if you will not use them again. Cut up old credit cards before discarding.
- Carry only the credit cards you plan to use.
- When you have applied for a new credit card, keep your eye on the mail and the calendar. If the card does not arrive within the appropriate time, call the credit card company.
- Do not use your mother's maiden name as a password for accounts. Make one up.
- Unless your mailbox is secure, mail payments at the post office and pick up new checks at your bank.
- If you are not interested in pre-approved credit offers, opt-out using the telephone number in our resource section.



what to do if you have **become** a victim

Despite your best efforts to protect yourself, you have become a victim. Now what? The following steps should be taken immediately and at the same time to be' 'nsure your protection.

Record Keeping

In the process of resolving the theft of your identity, be sure to keep records of all correspondence with the creditors and government agencies you contact. Include the date and name of contact. Follow up all telephone contacts with a letter and keep a copy.

Creditors

Notify all creditors and financial institutions, in writing and by phone, that your name and accounts have been used without your permission. If an existing account has been stolen, ask the creditor or bank to issue you new cards, checks and account numbers. Carefully monitor the account activity on your statements. Report fraudulent activity to the issuing company immediately. The Fair Credit Billing Act (FCBA) is a federal law that limits a consumer's responsibility for fraudulent charges to $50.

Local Law Enforcement

Immediately report the crime to local police. Provide them with as much documentation as possible. Make sure that the accounts are listed on the police report. Also, get a copy of the police report. Credit card companies, banks and credit reporting agencies may require you to show a police report to support your claim that a crime was committed.

Federal Law Enforcement

Report the crime to the Federal Trade Commission (FTC). The FTC collects complaints about identity theft from consumers and stores them in a secure online database called the Consumer Sentinel that is available to law enforcement agencies worldwide. The FTC provides information on ways to resolve problems resulting from identity theft and refers individuals to various private and government agencies for further action.

Federal Trade Commission Consumer
Response Center
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
1-877-IDTHEFT
www.consumer.gov/idtheft

The Credit Reporting Agencies

Contact the fraud units of the three credit reporting agencies: Equifax, Experian and Trans Union. Ask them to place a fraud alert on your credit report to help prevent new fraudulent accounts from being opened. Keep track of when it expires so you can ask for another one, if necessary. However, not all creditors check your credit report before issuing a new account.

As an ID fraud vicitm, you are entitled to a free copy of your credit report. Also, ask the agencies for a copy of your credit report every three months once you have become a victim. This can help determine how many

and which accounts listed are fraudulent. You can also identify the existing accounts that have been stolen.

Equifax 1-800-685-1111
www.equifax.com

Experian 1-888-397-3742
www.experian.com

Trans Union 1-800-916-8800
www.transunion.com

To opt-out of receiving pre-approved credit card offers, call 1-888-5-opt-out.

Utility Companies

Ask utility companies (local and long distance telephone se· providers, gas, electric and water companies) to w. out for anyone ordering services in your name. If someone has ordered services in your name, cancel those accounts. If you are having trouble with falsified accounts, contact your state Public Utility Commission.

Other Resources

United States Postal Inspection Service (USPIS)

The USPIS is a federal law enforcement agency that investigates cases of identity theft. The agency has primary jurisdiction in matters involving the integrity of the U.S. mail.

U.S. Postal Inspection Service
475 L'Enfant Plaza
Washington, DC 20260
202-268-2284
www.usps.gov/websites/depart/inspect/

United States Secret Service (USSS)

The USSS is a federal agency that investigates financial crimes. Generally, the USSS will intervene only when the dollar amount of the crime is high. However, they should still be notified in case it is part of a larger fraud ring.

U.S. Secret Service
Contact your local field office.
www.ustreas.gov/usss

Social Security Administration (SSA)

If you detect fraudulent use of your social security number, report it to the SSA. The SSA does not generally take action unless there is a high dollar amount, workplace impersonation or crimes committed in your name. They will only change your SSN if you fit their fraud victim criteria.

Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235
1-800-269-0271 (fraud hotline)
www.ssa.gov/

Call For Action, Inc.

Call For Action, Inc. is an international nonprofit network of consumer hotlines. CFA volunteers provide assistance and mediate cases on behalf of consumers and small businesses. For the office nearest you, refer to the back of the brochure. For more information on identity theft visit *www.callforaction.org.*

additional steps to take:

If your **bank accounts have been tampered with,** close those accounts, destroy any checks and cut up any ATM cards. Ask for password protection when opening new accounts.

ur **checks have been stolen or misused,** stop payment on all checks. Open a new account and reissue checks to legitimate creditors. Also, ask your bank to notify its check verification company to stop giving approval for any of the stolen checks.

If you believe your **investments or brokerage accounts have been tampered with,** report it to your account manager and the Securities and Exchange Commission.

Even if you think a problem is resolved, **check your credit report every six months** for several years after your identity was stolen.

If you suspect your **name and SSN are being used by** an identity thief to get a driver's license or non-driver's ID card in your name, contact your Department of Motor Vehicles.

Call For Action, Inc. (CFA) is an international nonprofit network of consumer hotlines affiliated with local broadcast partners. Help is available to individuals and small businesses. The Call For Action offices are:

WTAJ-TV
Altoona, PA
(814) 944-9336

WXIA-TV
Atlanta, GA
(678) 422-8456

WBZ Radio
Boston, MA
(617) 787-7070

WIVB-TV
Buffalo, NY
(716) 879-4900

WJW-TV
Cleveland, OH
(216) 578-0700

KKTV-TV
Colorado Springs, CO
(719) 457-8211

KTVT-TV
Dallas/Fort Worth, TX
(877) TEXAS11

WXYZ-TV & WJR Radio
Detroit, MI
(248) 827-3362

WINK-TV
Fort Myers, FL
(941) 334-4357

WFMY-TV
Greensboro, NC
(336) 680-1000

KCTV5
Kansas City, MO
(913) 831-1919

WTMJ-TV
Milwaukee, WI
(414) 967-5495

WABC Radio
New York, NY
(212) 268-5626

KPNX-TV, KNAZ-TV &
The Arizona Republic
Phoenix/Flagstaff, AZ
(602) 260-1212

WTAE-TV
Pittsburgh, PA
(412) 333-4444

KTVI-TV
St. Louis, MO
(636) 282-2222

KTVX-TV
Salt Lake City, UT
(801) 908-0444

WTOL-TV
Toledo, OH
(419) 255-2255

WTOP AM & FM
Washington, DC
(301) 652-4357

NETWORK HOTLINE
(All other areas)
Bethesda, MD
(301) 657-7490

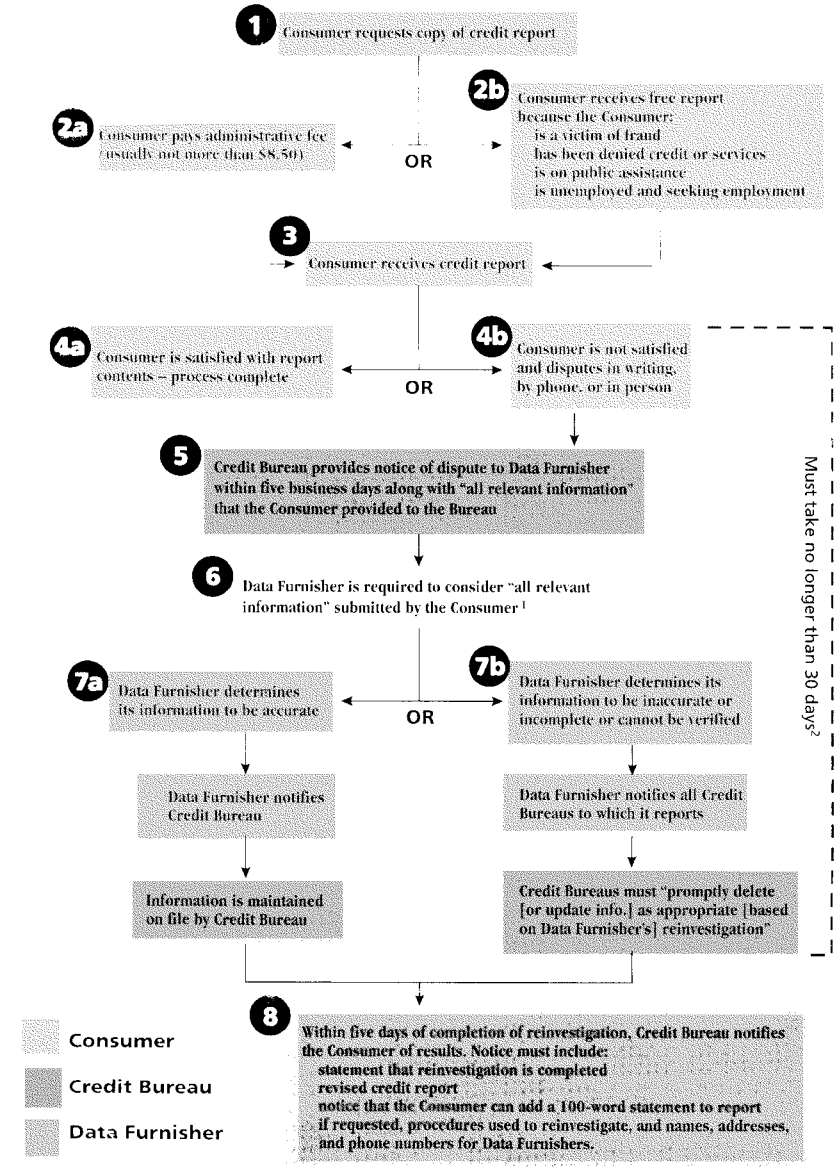
INTERNATIONAL
Radio Cultura
Buenos Aires, Argentina

Call For Action Headquarters
5272 River Road, Suite 300, Bethesda, MD 20816
(301) 657-8260
www.callforaction.org

2509 S. Stoughton Rd., Suite 300
Madison, WI 53716-3319
(608) 663-5000 – FAX (608) 663-50
www.cbmfoundation.org

Produced in cooperation with Associated Credit Bureaus, Inc.

Summary of Procedures for Disputing the Accuracy of a Credit Report



[1] Federal law prohibits Data Furnishers from reporting information to a Credit Bureau if the Data Furnisher has actual knowledge of the inaccuracy of the information. Federal law further prohibits Data Furnishers from providing disputed information to Credit Bureaus unless it also notifies the Bureaus that such information is in dispute.

[2] The process cannot take more than 45 days when the Consumer forwards additional information to the Credit Bureau.

© Copyright 2000 Associated Credit Bureaus, Inc.

Helpful Terms

The following terms are helpful in understanding the dispute resolution procedures flowchart:

Credit Reporting Agency. A credit reporting agency (also known as a credit bureau) is a company that maintains consumer credit information. The three main credit reporting systems in the United States are Equifax, Experian, and Trans Union. There are many local credit bureaus, as well you may find your local bureau in the phone book. Credit reporting agencies provide credit information to banks, credit card companies, lenders, or others when you apply for credit. Credit reporting agencies do not determine whether you will be granted credit or at what interest rate; they merely provide the information necessary to enable a credit grantor to make a lending decision.

Data Furnisher. A data furnisher is a person or company that provides your credit data to a consumer reporting agency (also known as a credit bureau). A data furnisher can be a credit card company or a bank that services your mortgage, car loan, student loan, or other loan. A data furnisher can also be a collection agency or a court clerk that provides information on liens, judgments, and bankruptcies.

Credit Grantor. A company or person that grants credit, such as a bank or retailer.

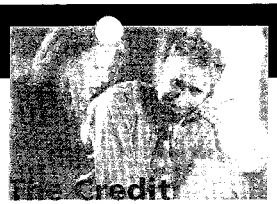
To Request a Copy of Your Credit Report

Equifax 1-800-685-1111
Experian 1-888-397-3742
Trans Union 1-800-888-4213
Consult a phone book for your local credit bureau.

To opt out of receiving pre-approved credit card offers, call 1-888-5-OPT-OUT.

© Copyright 2000 Associated Credit Bureaus, Inc.
E-24

Associated Credit Bureaus
1090 Vermont Avenue, NW
Suite 200
Washington, DC 20005



The Credit Reporting Dispute Resolution Process

The federal Fair Credit Reporting Act (FCRA) governs credit reporting agencies, also known as credit bureaus, as well as credit grantors and data furnishers. If you dispute the accuracy of any piece of information in a credit report, you can dispute that information directly with a credit reporting agency. Once a dispute is received by a credit reporting agency, the credit reporting agency and the data furnisher must follow certain procedures to reinvestigate that dispute in a set period of time.

The flowchart on the inside of this brochure is designed to help you better understand the dispute resolution process and contains definitions of important terms that will better aid the reading of the flowchart. This brochure contains helpful hints for avoiding a common credit scam credit repair. Finally, this brochure will direct you to two important resources where you can go for further information about credit reporting.

Associated Credit Bureaus

Associated Credit Bureaus

Associated Credit Bureaus (ACB) is the national trade association that represents credit reporting and mortgage reporting companies, as well as residential and employment screening companies and collections agencies.

For more information:

Associated Credit Bureaus
1090 Vermont Avenue, NW, Suite 200
Washington, DC 20005
(202) 371-0910
http://www.acb-credit.com

Federal Trade Commission
601 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
http://www.ftc.gov

Beware of Credit Repair Scams

If you wish to dispute an item on your credit report with a credit reporting agency, you are entitled to do so for free. A credit reporting agency will reinvestigate the dispute for free and, if applicable, issue you a revised credit report for free.

Credit repair organizations often promise to remove accurate information for a fee. But the Federal Trade Commission says, "the truth is, they can't deliver . . . Everything a credit repair clinic can do for you legally, you can do for yourself at little or no cost."

If you choose to use a credit repair agency, the organization must comply with the Credit Repair Organizations Act and must issue a disclosure document and a written contract to you. Further, they cannot request a fee in advance of services rendered. Finally, because the FTC says that "self help may be the best help," you should consider checking with the FTC before you use a credit repair organization.

Senator CRAIG. Now, I am going to turn to Dennis Carlton. Dennis is Director of Washington Operations for the International Biometric Group in Washington, DC. Dennis.

STATEMENT OF DENNIS CARLTON, DIRECTOR OF WASHINGTON OPERATIONS, INTERNATIONAL BIOMETRIC GROUP, LLC, WASHINGTON, DC

Mr. CARLTON. Senator, thank you, and on behalf of our company, I would like to thank the committee for the opportunity to talk to you about the technology called biometrics and describe how it can be used to combat the problem of identity theft.

Let me begin with a brief description of the International Biometric Group so that you better understand who we are and our unique position in the world of biometrics. International Biometric Group, or IBG, provides independent consulting services to government and private industry customers interested in biometric technology. Our organization focuses on three primary functions: Evaluating and reporting on biometric products and vendors, as well as the markets in which they compete; advising clients on how to implement biometric systems; and integrating a wide range of biometric hardware and software to meet the security needs of our customers.

We take a practical, hands-on approach to biometrics. We have conducted extensive comparative testing of more than 30 different biometric solutions so that we know how they are likely to perform in the real world. IBG holds to a strict vendor-neutral policy, which enables us to maintain close relationships with biometrics vendors while ensuring that our clients receive accurate and independent advice on which biometrics systems can best meet their needs.

Let me take a few moments to review some of the basics of biometrics. A technical definition of biometrics is the automated measurement of behavioral or physiological characteristics of a human being to determine or authenticate their identity. In other words, it is the use of computers to confirm who a person is by matching a behavior or a permanent physical characteristic with similar records in a database.

Research has shown that behaviors, such as the way we speak, the way we sign our names, and even the way we type on a keyboard, are distinct and unique enough that they can be quantified and compared by computers to existing samples. In a similar way, physical characteristics of the human body, such as the friction ridges on the pads of our fingers, the geometry of our hands, the shape of our face, and the patterns of our irises and retinas, can be measured and matched against computer databases.

A wide range of products on the market can acquire and match a person's biometric data in order to quickly and accurately identify who they are. Time permitting, I hope to be able to demonstrate some examples of these technologies to you later.

To effectively describe how biometrics can be used to combat identity theft and protect senior citizens, I think it is important to address some issues that often confuse the dialog about biometrics. First, it is important to set practical expectations of what biometrics can and cannot do. To date, we have not seen a biometric product that will work accurately 100 percent of the time. Whether

it is wrongly identifying one person as somebody else, only to identify someone it should not recognize, or preventing someone from initially enrolling in the system, all biometrics systems make errors. A properly designed system needs to employ biometrics as just one of a number of interlocking layers within a security solution and must also include a quick and efficient exception handling process.

Second, no one biometric technology is right for every application. For instance, while a finger scan technology may be an excellent solution for replacing passwords to gain access to a desktop computer system, it is not of much help trying to pick a potential terrorist out of a crowd in an airport terminal.

Finally, people should not automatically conclude that the use of biometrics is an invasion of our personal privacy or a violation of our civil liberties. Biometrics themselves are privacy neutral. It is the way they are employed and the protections put in place to limit misuse that makes biometrics either private invasive or privacy protective. What is essential is that individuals are fully informed on how their data is shared, used, collected, and secured. For more information about biometrics and privacy, I commend to you an IBG-sponsored website dedicated exclusively to the subject, www.bioprivacy.org.

Biometric technology has been employed to prevent fraud and identity theft for several years now. I personally managed a pilot program that began in 1998 which evaluated the use of finger scan technology in a retail grocery store for confirming the identity of people who paid for their purchases by personal or payroll check.

Reaction to the system by those who used it was universally positive. People found it much easier and faster to identify themselves with an index finger rather than digging through a pocket or purse for an ID, and the store found the incidence of loss due to check fraud reduced to zero. Most interestingly, senior citizens were some of the most enthusiastic proponents of the system. They recognized that no one could steal their checkbook and drain their bank account if a system like this was widely deployed.

Several companies have now commercialized the concept of identification at the point of sale, and I have brought some current examples of these technologies for demonstration purposes.

To properly serve the needs of elderly citizens, it may be necessary to make some adjustments to standard biometric systems. For example, the aging process can reduce the suppleness of a person's skin, which can present problems for finger scan technology. The use of certain moisturizers and specially designed sensors can significantly reduce this problem.

Another problem commonly associated with the aging process, decreased visual acuity, can make it difficult for people to properly position themselves for a facial scan or iris scan system. To overcome this challenge, vendors can offer more sophisticated camera systems that automatically locate the subject's face or eyes with little user effort.

As I mentioned earlier, for citizens who are physically unable to interact with the biometrics system, an efficient and transparent exception handling process is essential.

In conclusion, biometric technologies have already been shown to be powerful tools for combatting the growing scourge of identity theft that afflicts Americans, young and old. Thank you for your time, and I welcome the opportunity to demonstrate some of these technologies if time is available.

Senator CRAIG. Dennis, I will question you by allowing the demonstration at the end. How is that?

Mr. CARLTON. That is great, sir.

[The prepared statement of Mr. Carlton follows:]

Biometrics and the Prevention of Identity Theft

Testimony of
Dennis Carlton
Director of Washington Operations
International Biometric Group, LLC

To the

Senate Special Committee on Aging
July 18, 2002

My name is Dennis Carlton and I am the Director of Washington Operations for International Biometric Group of New York City. On behalf of our company, I'd like to thank the committee for the opportunity to talk to you about the technology called biometrics and describe how it can be used to combat the problem of identity theft.

Let me begin with a brief description of International Biometric Group so that you better understand who we are and our unique position in the world of biometrics. International Biometric Group, or IBG, provides independent consulting services to government and private industry customers interested in biometric technology. Our organization focuses on three primary functions: (1) evaluating and reporting on biometric products and vendors, as well as the markets in which they compete, (2) advising clients on how to implement biometric systems, and (3) integrating a wide range of biometric hardware and software to meet the security needs of our customers. We take a practical, hands-on approach toward biometrics. We have conducted extensive comparative performance testing of more than thirty different biometric solutions so that we know how they're likely to perform in the real world. IBG holds to a strict vendor-neutral policy, which enables us to maintain close relationships with biometrics vendors while ensuring that our clients receive accurate and independent advice on which biometric systems can best meet their needs.

Let me take a few moments to review some of the basics of biometrics. A technical definition of biometrics is the automated measurement of behavioral or physiological characteristics of a human being to determine or authenticate their identity. In other words, it's the use of computers to confirm who a person is by matching a behavior or a permanent physical characteristic with similar records in a database. Research has shown that behaviors such as the way we speak, the way we sign our names, and even the way we type on a keyboard are distinct and unique enough that they can be quantified and compared by computers to existing samples. In a similar way, physical characteristics of the human body such as the friction ridges on the pads of our fingers, the geometry of our hands, the shape of our face, and the patterns of our irises and retinas can be measured and matched against computerized databases. A wide range of products in the market can acquire and match a person's biometric data in order to quickly and accurately identify who they are. Time permitting, I hope to be able to demonstrate some examples of these technologies to you later.

To effectively describe how biometrics can be used to combat identity theft and protect senior citizens, I think it's important to address some issues that often confuse the dialog about biometrics. First, it's important to set practical expectations of what biometrics can and can't do. To date, we have not seen a biometric product that will work accurately 100% of the time. Whether it's wrongly identifying one person as somebody else, failing to identify someone it should have recognized, or preventing someone from initially enrolling in the system, all biometric systems make errors. A properly designed system needs to employ biometrics as just one of a number of interlocking layers within a security solution, and must also include a quick, efficient exception handling process. Secondly, no one biometric technology is right for every application. For instance, while a finger-scan technology may be an excellent solution for replacing passwords to gain access to a desktop computer system, it isn't of much help trying to pick a potential terrorist out of a crowd in an airport terminal. And finally, people should not automatically conclude that the use of biometrics is an invasion of our personal privacy or a violation of our civil liberties. Biometrics themselves are privacy neutral – it's the way they are employed, and the protections put in place to limit misuse, that make biometrics either privacy-invasive or privacy-protective. What is essential is that individuals are fully informed on how their data is shared, used, collected, and secured. For more information about biometrics and privacy I commend to you an IBG-sponsored website dedicated exclusively to the subject, www.BioPrivacy.org.

Biometric technology has been employed to prevent fraud and identity theft for several years now. I personally managed a pilot program that began in 1998 to evaluate the use of finger-scan technology in a retail grocery store for confirming the identity of people who paid for their purchases by personal or payroll check. Reaction to the system by those who used it was universally positive. People found it much easier and faster to identify themselves with their index finger rather than digging through a pocket or purse for an ID, and the store found the incidence of loss due to check fraud reduced to zero. Most interestingly, senior citizens were some of the most enthusiastic proponents of the system. They recognized that no one could steal their checkbook and drain their bank account if a system like this was widely deployed. Several companies have now commercialized the concept of identification at the point of sale; I've brought some current examples of these technologies for demonstration purposes.

To properly serve the needs of elderly citizens, it may be necessary to make some adjustments to standard biometric systems. For example, the aging process can reduce the suppleness of a person's skin, which can present problems for finger-scan technology. The use of certain moisturizers and specially designed sensors can significantly reduce this problem. Another problem commonly associated with the aging process, decreased visual acuity, can make it difficult for people to properly position themselves for a facial-scan or iris-scan system. To overcome this challenge, vendors can offer more sophisticated camera systems that automatically locate the subject's face or eyes with little user effort. As I mentioned earlier, for citizens who are physically unable to interact with the biometric system, an efficient and transparent exception handling process is essential.

In conclusion, biometric technologies have already been shown to be powerful tools for combating the growing scourge of identity theft that afflicts Americans young and old. Thank you for your time and I welcome the opportunity to demonstrate some of this technology to you.

Senator CRAIG. Let me turn to our other panelists for some questions.

Mari, obviously, you have been out on the front line, not only a victim, but assisting victims and helping them. Who can an elderly person go to to help them recover lost assets or fix damaged credit histories? Who can they turn to?

Ms. FRANK. Right now, there really are not many places. There are some legal aid places. There are some consumer agencies. But, in effect, there are not many places for people to go. I mean, you look at John Steven's cost. Then there are attorneys but not many will not take the cases on contingency. The FTC will just give you advice, like Mr. Beales said. So there really are not a lot of places that people can go unless people like me, who do pro bono work or if they get my kit. It is really an unfortunate thing. One of the suggestions that I had was that States and maybe the Federal Government set up some kind of an ombudsman center for help for people who really need it.

Senator CRAIG. Do you know if State Legal Aid Services assist seniors?

Ms. FRANK. Some of them do, yes, and there are some senior citizen programs around the country, and maybe AARP refers. But there is not anything really around—I have tried to refer people to others who will do the work for them and they come back to me, so that has been a problem.

Senator CRAIG. Thank you.

Boris, are bank tellers typically trained to spot the signs when someone is trying to access an account under a false ID?

Mr. MELNIKOFF. Yes. In fact, a lot of the training information I shared earlier in my testimony covers not only that, but also the unusual transactions that a senior citizen might want to conduct, which I think is an important factor. There have been many, many instances where a senior citizen would come into a bank, approach a teller. The teller will recognize the senior and the senior will want to withdraw large sums of cash. All of that—and it is preventable, and a majority of banks do exercise all of their rights to protect that consumer's assets, if you will. So the answer on both parts of the question, Senator, is yes. Bank tellers are trained to accomplish that.

Senator CRAIG. Do financial institutions have the authority to report suspicious financial activity that looks like identity theft to local authorities?

Mr. MELNIKOFF. Yes, sir. Through the use of a SAR, if you will, and additionally, here again, reverting back to the elderly or senior citizen withdrawing large sums of money, law enforcement in some instances is notified at once in the hopes of talking the senior citizen out of removing that kind or those dollar limits. In nine out of ten cases, it is nothing but a flim-flam that the senior is about to experience. So, yes, sir, your answer is, yes, we do do that as an industry.

Senator CRAIG. How do you effectively screen, because we have obviously heard of those who are making applications for purchasing cars using false IDs, a failure on the part of that loan officer to make a few simple calls to double-check addresses or anything of that nature? Is there any effort underway to double-check, re-

check, if you will, this kind of informational flow that would establish a credit and, therefore, allow a transaction to occur?

Mr. MELNIKOFF. Yes, and I think just to tie in with the announcement made by Treasury yesterday, if you will, that possibly would give the financial industry access to certain data as it pertains to the individual in the Social Security system. As we speak today, we do not have that ability to do so. We rely on, and I hope my colleague does not take any personal affront to this, but we rely on the credit bureaus and other systems for verification. But as mentioned earlier, the Colonel's date of birth or his Social Security number was issued prior to his birth. So we need to work on that, and by having access for legitimate reasons, that would be a significant help to the financial industry and to verify and reverify what we are doing.

Senator CRAIG. With the industry having to eat the cost once discovered, is there an annualized cost that identity theft is costing the banking industry of this country? Do you know of one that has been calculated?

Mr. MELNIKOFF. No, sir. There is no central repository. Now, there were statements made earlier, and I made a statement with respect to filing a SAR. But there are limits on the SAR, and the limits are $5,000 up to $25,000. So there is no central repository, so we really do not know.

But I think, and my opinion is, if you take all of the fraud that the financial industry, to include all types of credit grantors, we are probably looking at anywhere from $15 to $18 billion a year. That is on one side only. Then coupled with the other frauds, be it insurance fraud, Medicaid fraud, government fraud, with due respect, you are talking about another $10 to $15 billion. So fraud costs this nation a significant amount of money and I think we can do a much better job if we are allowed the tools or access to the tools to do it.

Senator CRAIG. It sounds like precautionary training and devices to detect and double-checking would be a rather inexpensive way of solving some of those problems.

Mr. MELNIKOFF. It certainly would, sir, and we support it.

Senator CRAIG. Mari, I saw your hand come up. Yes?

Ms. FRANK. Yes, sir. Thank you so much. One of the things that the Postal Inspector did for verification of addresses—this was after we complained about this in 1998 when I testified before the Technology Committee for the new Identity Theft Deterrence Act—was they started sending verification of address. So if you put in for a change of address, they now will send a postcard to the old address and the new address to see if you really have moved.

We have been asking the credit grantors and the banks to do the same, because—what has happened to John when he became a victim, what happened to me, the fraudster will always change the address. They have to do that so you do not find out about it. The main step that the creditors should be doing is when they see that the address that is on the application is different from the credit report, that should be a key signal that they should verify address with either a phone call or a postcard before they issue credit, and I have been asking for this for 6 years and I do not see this happening now with the creditors.

Senator CRAIG. Well, that is a great lead-in comment, Stuart, to turn to you. Mr. Pratt, do the credit reporting companies have the authority to report suspicious financial activities that look like ID theft to local authorities.

Mr. PRATT. We do not have any law like the one that permits banks to permit, under the SAR, the system of SARs. I think maybe the key question is, do we have the kind of information that would allow us to even identify something suspicious? We are loading an enormous amount of information per month into the databases and so there is almost every variation on a theme in terms of how files behave, if you will. Some people have very little credit. Some people accumulate very little credit over long periods of time. Other folks move frequently, so is an address change an indication of a problem? Is a couple of new credit accounts an indication of a problem?

So it may be a little bit difficult for us to pin down and say, aha, this one looks suspicious relative to the 200 million files we maintain, relative to the two billion items of information updated every month over the course of any given year, but we do not have an official authority to do so, no.

Senator CRAIG. You did indicate to me, though, that certain activities cause you to trigger an account, or what was the term you used in blocking an account or——

Mr. PRATT. Well, when a police report is submitted to us——

Senator CRAIG. When a police report is submitted.

Mr. PRATT. Yes, sir. Then we do use that as a way to escalate service for the consumer who is a victim. It is a way for us to——

Senator CRAIG. Only in that instance, then?

Mr. PRATT. Only in that instance, because today, with the technology that is out there, if we cannot use a police report, almost anyone can produce an affidavit. There is an awful lot of what we call credit repair, fraudulent credit repair activity, which is a process by which a firm may charge a consumer hundreds of dollars to then write letters and try to delete accurate but adverse information off the credit files.

So we have to have a way to distinguish between someone who simply wants to eliminate important risk data for safety and soundness of the banking system and someone who genuinely says, I am a victim of a crime, help me quickly, help me now, and that is what we do with the police report. That may not be the final answer, but that is our answer today, is to say a police report seems like a reasonably safe and sound process—although, by the way, do not miss that a fraudulent police report can be produced and we have already received fraudulent police reports.

Senator CRAIG. I would think that if they can steal IDs, they could steal a form and manufacture police reports that look fairly legitimate.

Mr. PRATT. It is hard to distinguish real and falsified documents of all kinds, and that is always the struggle for the industry.

Senator CRAIG. Then there is no reason in your mind to believe that a change of address is something that would trigger a response to check to see if that was a legitimate change, or is that simply going to be too costly for your——

Mr. PRATT. I do not think we are putting cost as the only metric out there to measure a decision that we ought to make that would help our system stay accurate——

Senator CRAIG. Well, I asked that—that was a legitimate question, where you get hundreds of millions of data——

Mr. PRATT. Let me put address changes——

Senator CRAIG [continuing]. You have got, therefore, probably hundreds of thousands of requests for address changes a year——

Mr. PRATT. In fact, it is millions——

Senator CRAIG [continuing]. It does cost to verify.

Mr. PRATT. We receive, because of the—and this goes actually to some of the Postal Service information as well as information from Census—about 40 million addresses change every year in this country. So it is difficult to use an address on its own as an indicator.

Also, many consumers on their credit file will probably have or may have more than one accurate address. I may use one card for my business purposes and so I may use my corporate address for that particular credit card. So that billing, that report that comes in every month from that particular lender shows my business address. Many of my other cards may be my home address, and so I may even have two legitimate addresses which are reporting into the system.

So admittedly, it is tough to pin it down and say, aha, this one is unique and this one deserves some different kind of attention.

Senator CRAIG. What would be some of the unintended consequences of overly broad restrictions on the use of Social Security numbers on credit reporting companies?

Mr. PRATT. For us, we have the Fair Credit Reporting Act that says you must maintain reasonable procedures to assure maximum possible accuracy. That was the law that Bill Proxmire passed back in 1970.

Consumers have several expectations at the table at any given time. One is, I want my information safe. Clearly, another one is, I also want it to be accurate. My credit report is, in large part, how I get my mortgage and how I do drive away with my car and how I obtain credit and so on and so forth.

So with 40 million address changes a year, with what we estimate to be about three million last names changing in this country due to marriage and divorce, with consumers sharing very similar last names—for example, there are about 2.5 million Smiths in this country and another two million Jones in this country, and so with consumers with very straightforward, very common last names, to keep that information separate, the SSN plays a very, very important role in the data accuracy, the data matching part of how we build our databases.

So it really depends on the approach taken to restricting the SSN, whether it directly applies to our business model or the members that we represent or whether it applies more generally out in some other dimension.

Senator CRAIG. Stuart, you heard Mr. Stevens testify this morning. I am aware that you are familiar with his case to some degree. Could you please tell me or the committee the status of that case at this moment?

Mr. PRATT. I have committed to Mr. Stevens, and I have to follow up with him to make sure I understand where he is in the process, particularly in light of the fact that there apparently is another account that showed up on his file. I have to know which of the systems it showed up on. I have to see whether it showed up in all three and then we will obviously follow up with him further.

One of the points, though, that Colonel Stevens made which is important to us, as well, and we will have to understand this better, is if the account is being cycled through collection agencies, the account number is not necessarily always reported to us, and so the question is, can the credit bureau—we want to keep that bad data off the file at all costs. There is nothing worse than sending to the customer, the American Bankers Association member, false information, because obviously they are making the wrong decision. They are missing out on a customer with whom they would like to do business, first of all.

So one of the technical questions, which we do not have to wade our way through here today, is, is there a collection reporting issue that we have to look into a little bit further based on Colonel Stevens' experience? But in terms of the specifics, obviously, I have made a commitment to Colonel Stevens to follow up with him and his wife and see where we are.

Senator CRAIG. That would be most helpful.

Mr. PRATT. Yes, sir.

Senator CRAIG. Before I go into this technology demonstration, Mari, I gave you the first word. I will give you the last word, if it is brief. [Laughter.]

Ms. FRANK. OK. Well, I guess I will say this about biometrics or Social Security number. I am going to pick up on this. Biometrics, or that piece of our body that we use as a unique identifier, in and of itself, it is not good or bad. It is how it is used.

The one thing I want to bring up that he mentioned was this, and this is the problem we are having with the Social Security number, if you use the Social Security number as the gateway or the key and you really do not spend a lot of time on other matching, like matching ages, birthdates, address, and you just focus on that Social Security number, you are going to get a lot of mismatches and a lot of errors and that causes that negligent information handling practices and fraud.

The same thing will happen with the biometric information. So if my fingerprint is used and somehow nothing else matches and there are these fraudsters and these techno-geniuses who can corrupt these files, and I have spoken with people in the Secret Service who have told me it can be done and I have read about it, so if someone is using a piece of biometric information instead of the Social Security number and there are still negligent information handling practices, meaning there are not matches, then if I become a victim at that point, how do I prove who I am?

So the issue of biometrics is the same as the issue of Social Security number. We have to take a broader look and have greater matching and verification. That is the issue. So I do not have a problem with biometrics per se just how it may be misused.

Senator CRAIG. I think I heard Dennis say, and I am about to be a victim of it, in a positive sense, that it is not 100 percent accu-

rate, and we understand it. But the application of it effectively creates a threshold that is important, I think.

I cannot disagree and I think there is one piece of information amongst many that have emerged out of the testimonies today, that checking and cross-checking and being cautious. Obviously, the message that—well, my wife and I just went through an experience about a year ago with the loss of her father and, therefore, working with her mother, and my wife is the trustee of the estate and working with her mother as an elderly person in Tucson.

Frankly, our relationship with the bank was very positive. They worked us over good when we went in with her mother to sit down and begin to work with her on her accounts and her investments, and it was a cross-check and a double-check. We were very pleased by that in the end. It was a threshold that we had to get through. In the first instance, there was almost an element of annoyance. Here is a daughter and a mother sitting down together, but the bank did not know that and other banks that they did business with wanted my daughter's signature and her presence there, so that was a little different.

But I was very pleased to see that, that there was a very real caution being taken there with this elderly person, because all of a sudden, here were two younger people who by all appearances were going to access potentially fairly large sums of money, so Boris, that was a pleasing experience.

I have not yet adjourned this committee. Dennis, what do you have in mind?

Mr. CARLTON. I have two demonstrations here, Senator, one of iris scan technology and one of finger scan technology to show you two different applications of how biometrics identifies an individual it knows and will reject someone that it does not recognize. So——

Senator CRAIG. How do I explain if my finger scan shows up on an FBI file? [Laughter.]

To my knowledge, that will not happen.

Mr. CARLTON. It will not here, Senator.

Senator CRAIG. All right, fine. I told staff, if I was going to subject myself to this and it was recorded on a CD, I got the CD. [Laughter.]

Let me come over and see what you have.

Thank you, panelists, very much for the testimony you bring and obvious experience that you have had on identity theft. The committee felt it was an important issue that we will continue to pursue and try to lift visibility, too, for the seniors of our country and, of course, if you lift it to seniors, you will lift it to others, because it is a growing concern, as we have said, nationwide, so we do appreciate that.

I am told that August 20 is National Senior Citizens Fraud Awareness Week. The Attorney General and Postmaster General will be speaking to that. I am pleased to hear that. It is obviously time that we continue on a progressive basis to publicize these issues, to draw public awareness to them.

I would like to insert in the record a statement submitted by Marc Rotenberg, Executive Director of the Electronic Privacy Information Center.

[The prepared statement of Mr. Rotenberg follows:]

Statement for the Record of

Marc Rotenberg,
Executive Director, Electronic Privacy Information Center
Carla Meninsky, EPIC IPIOP Fellow

Joint Hearing on
Identity Theft Involving Elderly Victims
Before the
Special Committee on Aging

United States Senate
July 18, 2002

Introduction

My name is Marc Rotenberg. I am the executive director of the Electronic Privacy Information Center (EPIC), a public interest research organization based here in Washington. I am also on the faculty of the Georgetown University Law Center where I have taught the Law of Information Privacy for ten years. Joining me in the preparation of this statement is Carla Meninsky, a student at George Washington Law School and an Internet Public Interest Opportunities Program (IPIOP) Fellow at EPIC.

We appreciate the opportunity to present this statement on the relationship between biometric techniques and the problem of identity theft. Identity theft imposes a significant cost on individual consumers. The primary cause of identity theft is the widespread use of the Social Security number as a record locator and individual identifier. Because of the absence of effective controls on the use of the Social Security numbers, SSNs are regularly marketed, stolen or counterfeited.

The problem of identity theft cannot be solved by widespread adoption of biometric identifiers. While there are currently over 20,000 military, government and commercial installations using some form of biometric identification, those installations are specific applications within small, controlled communities.[1] To create a nationwide network of biometric identification would be a huge undertaking, requiring vast amounts of storage and hundreds of million of dollars. It would not solve the identity theft problem, but it would raise new and difficult problems, particularly for the elderly.

We will briefly review how biometrics are used as identifiers, discuss some of the advantages and limitations of each of the biometrics available today, and make a few brief recommendations.

The Problem of Identity Theft

[1] Erik Bowman, *Everything You Need to Know About Biometrics*, Identix Corporation (Jan. 2000), http://www.ibia.org/EverythingAboutBiometrics.PDF.

Identity theft accounted for over 80 percent of Social Security number misuses reported to the Social Security Administration.[2] The cost of identity theft is expected to reach eight billion dollars by the year 2005.[3] However, this represents one tenth of a percent of the credit industry's income and only a small fraction of the amount of loss due to fraud and stolen credit cards. The average loss to the financial industry is $17,000 per identity loss, but the loss to the victim is potentially much greater.

Most victims of identity theft face significant credit bills and the destruction of their credit history. The immediate consequence could be the loss of securing a job or purchasing a home, or worse.[4] Other victims face arrest for crimes that an impersonator has committed in their name. If the arrest occurs, it may be impossible to cooredt. Identity theft has been used to obtain employment, drivers' licenses, receive government benefits, and evade criminal prosecution. Identity theft indirectly affects everyone because it causes interest rates to increase to cover the industry's losses.

While the majority of those reporting identity theft are between the ages of 20 to 40, identity theft is of particular concern to the elderly because of the length of time between when the theft occurs and when it is discovered. Usually it is more than a year later and only because much needed credit has been denied.[5] For people who may use credit cards infrequently, the delay between when the theft occurs and when the card is needed will further exacerbate the problem of correction. Identity theft also weighs heavily on those who have established good credit histories over a long period of time and then confront the challenge of correcting a credit statement in retirement.

Biometrics as a Solution

One approach to the problem of reducing the threat of identity theft is the widespread adoption of systems of biometric identification. Biometric identification systems are automated methods of recognizing a person based on one or more physical characteristics, such as fingerprints, voice, or facial characteristics. Computer-based pattern matching is at the core of all biometric systems. The technologies available are subject to varying degrees of error, which means that there is an element of uncertainty in any match.

The accuracy of biometric systems is measured by their *false acceptance* and *false rejection* rates. A false acceptance is when the wrong individual is matched to a stored biometric. A false rejection is when an individual is not recognized who should have been. The two measures are dependent. In reducing false acceptances, the false rejection rate will increase. Reducing false rejections will cause the false acceptance rate to go up. Most biometric systems adjust false acceptances or false rejections to the type of application and the amount of security required. High security areas, such as bank vaults

[2] Analysis of Social Security Number Misuse Allegations Made to the Social Security Administration's Fraud Hotline, Management Advisory Report, SSA (Aug. 1999).
[3] Identity Theft Complaint Data, Identity Theft Data Clearinghouse, Federal Trade Commission (2001).
[4] Statewide Grand Jury Report: Identity Theft in Florida, Case No. SC 01-1095 (Jan. 10, 2002).
[5] Id.

and military installations are protected by biometric systems that minimize fraudulent acceptances. The false acceptance rate must be low enough to prevent imposters, but as a result, people who rightfully should be accepted, are often refused. In these cases, human intervention is typically available to provide authentication when the biometric system fails.

Fraud occurs when either an imposter is trying to be accepted as someone else to gain entry or usurp funds, or when an imposter is trying to avoid being recognized as someone already enrolled in the system and tries to enroll multiple times. The first is a form of identity theft, the second creates multiple identities for a single individual. Both types of fraud must be safeguarded against in any biometric system, however, depending on the application, it may be reasonable to relax one criteria to prevent the other.

There is no perfect biometric system. Each type of biometric system has its own advantages and disadvantages, and must be evaluated according to the application for which it is to be used.

Creating and Using an Identity Database

There is a distinction between Authentication, Identification and Enrollment. Authentication is the easiest task for a biometric system to perform. Identification is more difficult and much more time consuming. The enrollment process determines the ultimate accuracy of the biometric system. A single biometric system can be created for identification or authentication, but not both, although the two applications can share the same database of biometric samples.

One-to-One Matching

Authentication answers the question, am I who I say I am? A person presents a biometric sample, and some additional identifying data, such as a photograph or password, which is then compared to the stored sample for that person. If the person is not an imposter, the two samples should match. This is known as a one-to-one match. If a nonmatch occurs, some systems retake up to three samples from the person to find a best match. This is the simplest task of a biometric system because the independent identifiers help to corroborate the individual. The biometric acts as a secondary password to protect the individual. Authentication of an individual takes at most a few seconds.

One-to-Many Matching

Identification means to answer the question, who am I? A person provides a sample biometric, sometimes without his knowledge, and the system must compare that sample to every stored record to attempt to return a match. This is known as a one-to-many match, and is done without any corroborating data. Because the matching process is based on the closeness of the new sample to a stored sample, most systems return a likely list of matches. Others return a single match if the sample is similar enough. The time for the result depends on the size of the database. The FBI's Integrated Automated

Fingerprint Identification System (IAFIS), which is used to identify criminals, can perform over 100,000 comparisons per second, usually completing an identification in 15 minutes with a database of over 42 million records.[6] If identification must be done on a wide-scale basis, the number of comparisons that will need to be done simultaneously will be astronomical. In addition, consumers might be unwilling to wait more than a few seconds to be able to use their bank ATMs or on-line service.

Negative identification is when an individual can be accepted to receive a benefit only if he is not yet enrolled in a database, such as a government-run welfare program or drivers registry. Even negative identification is susceptible to fraud. A person already enrolled in the system can avoid being recognized by attempting to falsify his biometric or skew the data collection. Rejecting imperfect images in the enrollment process, improves the integrity of the database, but cannot solve all enrollment problems.

Entering a New Person into the Database.

Enrollment is the process of introducing a new person into the database. The person's biometric must be sampled and stored together with his or her identity. The greatest problem is there is no existing guarantee as to that identity. A biometric system can only be as good as the accuracy of any background information that is relied on. If fraudulent information is used to enroll an individual, through a fake birth certificate or stolen social security number, a biometric can only verify the person is who they said they were at the time of enrollment. One important enrollment test is to match every new person against all other entries to check for duplicate entries and possible fraud. Without this check, once a person is in the database, it will be impossible to trace an imposter assuming multiple identities.

What happens if a person cannot be enrolled?

There will always be a small percentage of users who cannot enroll in biometric systems either because they are unable to produce the necessary biometric—a missing finger or eye—or they are unable to provide a quality sample at enrollment. Others repeatedly cannot match their biometric to the stored template. These individuals will never be identified by the biometric system.

Since biometrics deteriorate with age, the elderly will be particularly affected. They will constitute the largest portion of those unable to enroll or be recognized by a biometric system. There needs to be an alternative solution for those who cannot be recognized by a biometric system so that they will not be denied rightful benefits.

Relying on Biometrics as Identifiers

The Legal Aspects of Biometrics

---

[6] *What Could Biometrics Have Done?*, *at* http://www.biometricgroup.com/e/Brief.htm (last visited Jul. 15, 2002).

No court has, as yet, permitted computer authentication of human identity. *United States v. Mitchell*[7] was the first case to question the use of latent fingerprints as evidence to identify an individual. The *Daubert*[8] standard, which is used to establish the reliability of an expert witness, requires that any method or technique must have been subjected to statistical analysis and its error rate must be known. Mitchell based his claim on the lack of objective testing for fingerprints and the actual error rate is unknown. Indeed the National Institute of Justice and the biometrics community are just now trying to establish standards for performing such testing. However, the Court ruled that fingerprints were accepted scientific methodology.

Experts in the field still contest the analysis on which the decision was based. Indeed, a subsequent case, *United States v. Plaza*, which relied heavily on the scientific testimony from *Mitchell*, initially disagreed with the *Mitchell* holding.[9] However, the Court later revised its opinion saying that the FBI error rate in fingerprint matching was not "unacceptably high."[10]

Uniqueness of biometric data is affected by time, variability and data collection.

The key to any biometric system is that the biometric being measured is unique between individuals and unchanging over time. Otherwise the stored biometric associated with an individual needs to be periodically updated. There are several factors affecting the accuracy of any identification. Biometric data collection can be affected by changes in the environment, such as positioning, lighting, shadows and background noise. But the biometrics of an individual are also susceptible to change through aging, injury and disease. Because of this, the accuracy of all biometric systems diminishes over time.

Collecting biometric data introduces errors in the data.

Any biometric sample, whether a fingerprint, voice recording, or iris scan, is not matched from the raw data. There is too much data to store and compare during each attempted match, especially if the sample needs to be transmitted to a central database for matching. Instead, biometric systems use templates. The raw data is simplified through feature extraction. Face recognition systems need the most number of features to be extracted and hand scans need the least. The extracted features are compressed further into a sample template which is then compared to a stored template to determine if there is a match. Information is lost with each level of compression making it impossible to reconstruct the original scan from the extracted points. Since even minor changes in the way a sample is collected can create a different template for a single individual, matches are based on probability. Systems are adjustable to the amount of difference they will

[7] *United States v. Mitchell*, 199 F. Supp. 2d 262 (E.D. Pa. 2002).
[8] *Daubert v. Merrell Dow Pharmaceuticals*, 113 S.Ct. 2786 (1993).
[9] *United States v. Plaza*, 179 F. Supp. 2d 492 (E.D. Pa. 2002).
[10] *United States v. Plaza*, 188 F. Supp. 2d 549 (E.D. Pa. 2002).

tolerate to confirm a match. The more independent the data available for matching, the more credible the match.[11]

Increasing the speed of biometric systems can introduce error

In extremely large populations, storage of templates is partitioned into characteristics, or bins, for ease of searching. These bins can be based on external characteristics such as gender or race, or they can be based on the biometric's internal characteristics. Traditional fingerprint identification has been based on the binning idea, with classifications based on whorls, loops and arches. Computerized systems take advantage of this concept. While binning can speed the time for identification and allows for better statistical matches within each bin, if a template is wrongly binned, it can never be found.[12]

Types and Accuracy of Biometrics

Fingerprint scanning is the best known and most widely used Biometric.

Fingerprints are the best-known and most studied biometric. Basic fingerprint technology has been around for over a century. Technically-sophisticated fingerprint scanners are available from $300 to just over $1,000, although an entire biometric installation can cost upwards of a million dollars. The FBI's IAFIS, which has cost several hundreds of millions of dollars, is 98% accurate with a database of over 42 million sets of ten-finger prints.[13] But fingerprint authentication systems still reject over 3% of authorized users when false acceptances are minimized.[14] Systems currently in use by state and local governments must use at least two-finger identification schemes in order to achieve that level of accuracy for much smaller populations, usually around a few hundred thousand people.[15]

Fingerprint patterns are created from the ridges on your fingers. The patterns, consisting of loops, whorls and arches, have been shown to be unique between people. Even on a single individual, each of the ten fingers has a different pattern. However, the ridges necessary to create the pattern age and deteriorate over time. Fingerprint templates are influenced by the pressure, position, and dryness of the finger on the scanner. Scars, calluses or cracks in the skin can change the template. While more sophisticated scanners can compensate for dirt or other contaminates, simple household cleaners can remove the ridges necessary to obtain a readable print. Even long fingernails can prevent a scanner

---

[11] James L. Wayman, *Generalized Biometric Identification System Model*, U.S. National Biometric Test Center, Proc. 31st IEEE Asilomar Conf. Signals, Systems and Computing (1997), http://www.engr.sjsu.edu/biometrics/nbtccw.pdf.
[12] James L. Wayman, *Large-Scale Civilian Biometric Systems*, U.S. National Biometric Test Center, Proc. CardTech/SecurTech Government (1997), http://www.engr.sjsu.edu/biometrics/nbtccw.pdf.
[13] Congressional Statement, 2000 - Crime Regarding HR 3410 and Name Check Efficacy , *at* http://www.fbi.gov/congress/congress00/loesch.htm (last visited Jul. 9, 2002).
[14] Bowman, *supra* note 1.
[15] *See* Wayman, *supra* note 9.

from correctly taking a fingerprint. Still, fingerprint technology is the most cost-effective biometric available today.

Retinal scans are the most accurate, but least acceptable to the public.

Retinal scans are the most accurate. They capture the pattern of blood vessels in the eye. No two patterns are the same, even between the right and left eye, or identical twins. Nor do retinal patterns change with age. The drawback to retinal scans is that typically the data capture process is also the most invasive. This makes them the most difficult to administer, thus making any sample subject to the most errors in data collection. To get a usable sample, an individual must cooperate by keeping his head fixed and focusing on a target while an infrared beam is shown through the pupil. The reflected light is then measured and captured by a camera. Retinas are also susceptible to diseases, such as glaucoma or cataracts, which would defeat a system intended to protect the elderly.[16]

Iris scans are accurate, less invasive, but not proven.

Iris scans are a fairly new technology that appears to be almost as accurate as retinal scans. The advantage over retinal scans is collection of the sample template is not as invasive: a video camera is used to take a picture of the iris. Cooperation of the individual is still necessary, though. The person must be within 19 to 21 inches of the camera and focused on a target in order to get a quality scan, although work has been done with inserting lenses to sharpen the sampled image. Movement, glasses and colored contact lenses can change the template created from a single individual. Eyelids and eyelashes obscure part of the surface of the iris. Since the scan is based on the size of the pupil, drugs dilating the eye could defeat an iris scan.

Iris patterns are thought to be unique. However, since the technology is fairly new, a large enough database has not yet been assembled to prove this assumption. The iris allows for the fastest comparisons against a database, checking 100,000 records of iris codes in two seconds, compared with 15 minutes for a fingerprint scan to do the same task.[17]

Face Recognition systems are the least reliable.

Face recognition is the least reliable of the biometrics available today. Lab tests by two of the nation's biggest testing centers, the Biometrics Fusion Center in West Virginia, run by the United States Department of Defense, and the International Biometric Group, a research and consulting firm in New York, show that correct matches are produced only about 54% of the time.[18]

---

[16] Bowman, *supra* note 1.
[17] John Daugman, *How Iris Recognition Works*, University of Cambridge, *at* http://www.cl.cam.ac.uk/users/jgd1000/ (last visited Jul. 9, 2002).
[18] *See* P. Jonathon Phillips et al, *An Introduction to Evaluating Biometric Systems*, Computer (2000), http://www.dodcounterdrug.com/facialrecognition/DLs/Feret7.pdf.

Face recognition is a difficult task, usually requiring a system to isolate an image in a complex environment and then to compare it to a stored template that was sampled in a controlled environment. Face recognition relies on matching the same head position and angle, so several poses need to be collected to create a single template. Light, shadows, facial expression, weight gain, and sunglasses all affect the system's ability to produce a match, oftentimes making mistakes across gender. Even when the sample is taken in a similar controlled environment to the stored template, face recognition systems have trouble matching to images that were stored more than one year earlier.[19] Research groups are now trying different approaches to improve face recognition systems.

Other biometrics are only accurate for smaller groups of people.

Other biometric products and research are available, with differing degrees of success: signature scanners, vein patterns, gait recognition are a few. However, most are inappropriate to identity protection. For example, hand readers are currently in use in many installations. However, because they contain the smallest dataset, and because hand geometry is neither time-invariant or unique, their effectiveness breaks down in large populations, producing too many duplicate matches. Hand readers can also be defeated by jewelry and weight gain.

Voice recognition is skewed by background noise, and whether an analog or cell phone is used. While it is impossible to fool a voice recognition system through impersonation or mimicry, it is possible to use a tape recorder to commit fraud.

Evading a Biometric System

There are several ways to try to circumvent a biometric system. False identification at enrollment, physically altering a personal biometric, skewing the sample collection by not cooperating, and hacking into or falsifying the database are all ways that biometric recognition can be compromised. Sample data could even be altered or stolen during transmission to a central database. How a biometric system is set up, protected and maintained will determine the effectiveness of the system.

One of the most often asked question is whether biometrics can be defeated by prosthetic devices. The best biometric scanners in use today detect a pulse or heat from the individual to make sure that the sample has come from a live human being.

Other Options Available to Prevent Identity Theft

Although biometric techniques provide a variety of methods to identify individuals, the best way to reduce the specific problem of identity theft is to reduce the use of the Social Security number as a record locator and personal identifier. States are now recognizing the source of the identity theft problem and have begun to enact

[19] William A. Barrett, *A Survey of Face Recognition Algorithms and Testing Results*, U.S. National Biometric Test Center, *at* http://www.engr.sjsu.edu/biometrics/nbtccw.pdf (last visited Jul. 15, 2002).

legislation protecting use of the Social Security number. In Georgia, businesses face fines of up to $10,000 for not protecting consumer personal data. California gives consumers a right to freeze their credit report, so that no business can access it without their consent. Florida, as part of a Grand Jury Report on Identity Theft, has recently recommended that Social Security numbers be prohibited from being used as identifiers unless required by law, and that both government agencies and individuals should be held accountable for releasing personal identifying information with public records.

Privacy Considerations

It is also important to recognize in the design of any system of biometric identification that the creation of a database linked to the individual and containing access to sensitive, personally identifiable information will create a new series of privacy issues. Administrators of these systems as well as those who gain access to these databases unlawfully will have access to personal information as if they were themselves the individual subject. It is conceivable that data could be altered either by administrators or by those who gain unlawful access to the database. The result would be records that wrongly indicate biometric authentication when in fact the subject did not engage in the event recorded. There are techniques to minimize these risks, but no system is foolproof.

It is also important to understand that once a biometric identifier is compromised, there will be severe consequences for the individual. It is possible to replace a credit card number or a social security numbers, but how does one replace a fingerprint, voiceprint, or retina? These questions need to be considered in the design and deployment of any system of biometric identification for a large public user base.

Conclusion

Biometrics identifiers will not solve the problem of identity theft facing the elderly community. Biometric systems in use now are successful because the number of people enrolled is limited. When the system fails, human administrators are available to assist in the authentication process. Creating an automated system on a national scale is beyond the capability of any of the existing technologies. Simply by merging the existing systems into a single central database would cause the reliability of those systems to be lost. Further, biometric databases are subject to new forms of abuse which may be more difficult to correct and will pose significant consequences for individuals whose biometric identifier is compromised. A less expensive approach to the problem of identity theft would be to reduce the disclosure and sale of the Social Security Number. It is the easy availability of the SSN that has contributed to the rapid growth in identity theft, particularly among the elderly, over the past decade.

Finally, we would like to draw your attention to the article on biometrics that appears in the current issue of Consumer Reports. The magazine concludes, "The nation urgently needs to tackle the complex task of regulating biometrics before vast stores of data are built." We wholeheartedly agree.

References

EPIC, Biometric Identifiers
http://www.epic.org/privacy/biometrics/

EPIC, Face Recognition
http://www.epic.org/privacy/facerecognition/

EPIC, National ID Cards
http://www.epic.org/privacy/id_cards/

Roger Clarke, *Biometrics and Privacy, at*
http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html (last visited Jul. 9, 2002).

Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues, at*
http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html (last visited Jul. 9, 2002).

James L. Wayman, *Fundamentals of Biometric Authentication Technologies*, U.S. National Biometric Test Center, San Jose State University (1999).

Sharath Pankani et al, *On the Individuality of Fingerprints*, Proc. Computer Vision and Pattern Recognition (2001), http://biometrics.cse.msu.edu/cvpr230.pdf.

Biometrics Research, Michigan State University, *at* http://biometrics.cse.edu (last visited Jul. 15, 2002).

Biometric Identification, San Jose State University, *at*
http://www.engr.sjsu.edu/biometrics/ (last visited Jul. 15, 2002).

"Your body, your I.D.?" Consumer Reports 12-13 (August 2002)

Contact

Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009
+1 202 483 1140 (tel)
+1 202 483 1248 (fax)
www.epic.org

HOME FRONT

Your body, your I.D.?

Iris scans, thumbprints, hand maps and other computer technologies may make us safer and more vulnerable at the same time.

Biometrics—automated identification gadgetry—was once the stuff of sci-fi movies. A hand placed on a pad would magically open a door on the planet Galaxos; or a scan of a face would trigger an alarm in the workshop of Despota, Duchess of Doom.

Now, however, such technologies are gradually becoming part of daily life. Children in more than a dozen school districts in Pennsylvania pay for lunch by placing a finger on a scanning pad. A computer recognizes each child and bills the appropriate account for the meal. Members of the San Antonio City Employees Federal Credit Union, in Texas, access safe-deposit boxes via hand scans. Casinos use face-recognition software to identify known cheats.

Biometrics' promise is to close the chinks in our personal- and national-security armor. By using biological traits that are unique to each individual, experts say, security systems will be able to distinguish people who are dangerous from those who are not, for example, and, potentially, to ascertain whether a person using a credit card is really entitled to do so.

But there is much in these new technologies to make consumers wary. For starters, material about our physical persons could be collected without our knowledge. Second, information residing in biometric databases may be misfiled or lost. Finally, once images like fingerprints or faces are turned into computer data, they become vulnerable to copying or theft.

FASTER THAN AN EYEBLINK

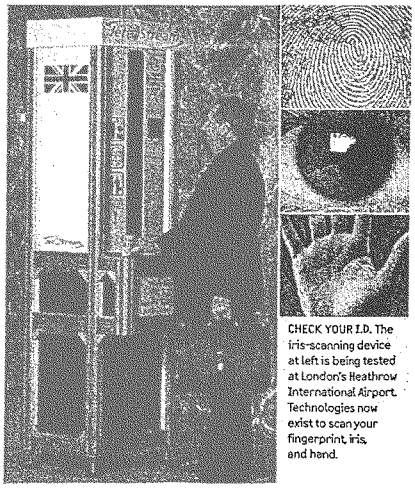
Biometric technologies have been gaining a place in security systems over the past 20 years. After the Sept. 11 terrorist attacks, however, they began to be widely promoted as the most efficient way to decrease our vulnerability to unwanted incursions of all kinds. Congress gave biometrics a further boost this spring when it passed legislation requiring biometric data to appear on all alien visa and travel documents by October 2004.

Biometric technologies bring several advantages to the task of identifying individuals—chief among them speed and accuracy. In a recent demonstration of biometrics at a conference in New Orleans, Bill Holmes, vice president of SSP Solutions, an Irvine, Calif., security software company, sat about 18 inches from what looked like a 4-inch-high stereo speaker—actually an iris-scanning device. After he pressed a key on his laptop, which directed the scanner to take a picture of his iris, software translated its unique pattern of flecks into an encrypted binary-code template. The program then compared it to a stored version of his own to see if he was who he claimed to be. In a wink the program matched his two iris portraits and granted him access to a restricted Internet site.

Biometrics can buttress the system of PINs and passwords already in place. While passwords allow access to your personal accounts by acknowledging that the numbers and letters are correct, they do not recognize the person who provided them. Hackers who obtain access data by scanning through millions of number and letter combinations to find one that works can steal money or even a person's identity.

By contrast, biometric data are unique to each individual. A scan maps enough key points to ensure that it is statistically unlikely for someone else to have the same pattern. That map would be fed into a digital template which would then be encrypted and stored on a portable carrier: a credit card, a personal digital assistant (PDA), your computer, or in a host database—your bank's, for example.

When you need to prove that you are you, a new scan is made of your eye, hand, or fingerprint and compared with a stored version. For greater safety, a security system could store biometric markers, along with PINs or passwords. "A backup system is always needed for the person who can't provide the required biometric," says Richard Norton, executive director of the International Biometric Industry Association.



CHECK YOUR I.D. The iris-scanning device at left is being tested at London's Heathrow International Airport. Technologies now exist to scan your fingerprint, iris, and hand.

BODY MARKERS

Some physical features lend themselves to mathematical representation more easily than others. Here's a rundown of the most common identifiers now in use. In the chart on page 13, you can find a guide to their uses and limitations.

Irises. A scan takes a digital picture of the patterns unique to each individual.

Fingerprints. A scanner collects 50 to 100 data points from a press pad, recording

patterns of ridges and valleys. The device can be built into a cell phone, a computer mouse, or a PDA.

Hands. Scanners use a video image and mirrors to measure distances between 80 different reference points and encrypt those measurements onto a tiny template. Dirt and cuts do not detract from performance.

Faces. Using a video camera, software maps and measures about 80 points across your face and then searches for a possible match with stored images.

Voices. With a spectrogram, a machine that measures the frequencies of speech, a biometric program creates a mathematical representation of your voice.

A CASE OF MISTAKEN IDENTITY?

The drawback to biometric technology is that its accuracy depends to a great extent on the government agency, company, or organization that uses it. Some software will update a person's mathematical template whenever a transaction is successfully completed, to keep up with any physical changes that occur with age or injury. Fingerprints, for example, become harder to read with changes caused by wrinkles and small scars. But currently, there is no standard to require all machines to provide such updating, and it is not clear whether the entities using biometrics will be willing to pay for that.

The general consensus among experts is that among the various techniques, iris scanning is the most accurate and face recognition is the most prone to incorrect matches. Moreover, all biometric methods, except iris scans, allow users to set a threshold for making a match. If this tolerance setting is tightened to make it harder for interlopers to gain access, it will in turn reject more authorized users. Conversely, if all authorized people can pass through easily, then it is more likely that an imposter will slip through, compromising the security the system is supposed to provide.

Unfortunately, there are no manufacturing, testing, or implementation standards for such thresholds. So one airport face-recognition system may let you catch your plane while the system at another airport might determine that you look enough like a terrorist to warrant detention.

There's also the possibility that a biometric identifier could connect you erroneously with a crime. Fortunately, there is no way to plant your fingerprint at a crime scene because the identifier represents only certain datapoints, not your entire print. "It would be like trying to make a whole potato out of mashed potatoes," explains Judith Markowitz, president of a Chicago consulting company that specializes in voice identification systems. Still, biometric information about you could conceivably be used to commit crimes. A shady company might make two I.D.s with your biometric data and sell one to a criminal.

YOUR PRINTS ALL OVER THE PLACE

"Earlier forms of technology, such as wiretaps, are subject to elaborate restrictions, but there has been little discussion about curbs needed for these high-tech devices," says Marc Rotenberg, director of the Electronic Privacy Information Center (EPIC), in Washington, D.C. Indeed, biometric devices can capture both your face and your voice without your consent and add them to a database that could be used elsewhere.

Even for fingerprint, hand, and iris scans, which require a person's permission to obtain, there is a measure of coercion if your state requires a fingerprint before giving you a driver's license, it's very unlikely you'll say no. Or if a would-be employer insists you provide an iris scan, you'll likely comply. Only in the area of commerce, where companies compete for customers, might consumers have leeway to opt out.

Another worry: Will biometric data be kept secure? Indivos, a developer of fingerprint technologies, reveals in its privacy statement that it may give anonymous biometric images to vendor partners for testing purposes. That may sound harmless, but, eventually, biometric data, just like other data, could be stolen and used on credit cards, licenses, and other documents, unless its guardians remain vigilant.

RECOMMENDATIONS

The nation urgently needs to tackle the complex task of regulating biometrics before vast stores of data are built. The International Biometric Industry Association says it supports privacy and testing standards to make sure that consumers are comfortable with the new security technologies. To do that, the industry, along with the federal government, will have to:

- Set standards of accuracy for all biometric devices.
- Limit data collected without consumers' consent.
- Inform consumers when their faces, fingerprints, voices, and the like are being captured by biometric scanners.
- Establish rules for the collection and maintenance of biometric databases and any possible reuse of biometric images.
- Provide for government oversight of data collection restrictions and safeguarding.

Biometrics in action

Already, biometric devices are installed at thousands of facilities across the nation. In addition to the limitations described below, the technologies can vary in their accuracy according to the sensitivity level the user sets.

TECHNIQUE	NOW USED TO I.D.	LIMITATIONS
Iris scanning	Travelers at Heathrow International Airport in London; the U.S. Office of Legislative Counsel, which drafts laws for Congress.	Some color-changing contact lenses may disrupt scan.
Fingerprint scanning	Drivers in Colo., Ga., Hawaii, Texas, and W.Va. Those states issue drivers licenses with bar codes that contain fingerprint templates.	Dirty or greasy fingers can make it hard to read the fingerprints. Match is hard to make when skin is unusually oily or dry.
Hand geometry	Walt Disney World annual pass holders; casinos in Atlantic City and Las Vegas.	May be difficult for people with conditions that affect flexibility, for example, chronic arthritis.
Face recognition	Drivers in Ill., W.Va., and Washington, D.C., who have the information embedded in bar codes on their licenses; Super Bowl ticket holders in 2001.	Hats, shadows, and changes in facial hair or hair styles can interfere with face recognition.
Speech recognition	Juveniles on probation in New York City who must check in with authorities.	Recognizing callers who use one kind of telephone to give a voice sample and then a different kind (say, a cell phone) to provide a match. Colds and laryngitis can also affect accuracy.

Senator CRAIG. Again, the committee thanks you all for your participation today and the committee will stand adjourned.

[Whereupon, at 11:49 a.m., the committee was adjourned.]