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