WRITTEN STATEMENT

OF

MICHAEL W. NAYLOR
DIRECTOR OF ADVOCACY
AARP

FOR THE HEARING ON

"THE GROWING PROBLEM OF IDENTITY THEFT AND ITS RELATIONSHIP TO THE FAIR CREDIT REPORTING ACT"

BEFORE THE

BANKING, HOUSING AND URBAN AFFAIRS COMMITTEE

UNITED STATES SENATE

JUNE 19, 2003
538 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, D.C.

FOR FURTHER INFORMATION, CONTACT:

ROY E. GREEN
FEDERAL AFFAIRS
(202) 434-3800

Good morning, Chairman Shelby, Ranking Member Sarbanes, and other distinguished Members of the Senate Banking, Housing and Urban Affairs Committee. My name is Michael Naylor. I am the new Director of Advocacy at AARP.

I want to take advantage of my first appearance before the Committee to introduce myself to you in my new role at AARP. I also want to take a moment to stress my strong desire to work closely with you on the full range of issues that come before this Committee which are of interest to our Members – and to midlife and older Americans generally.

Let me begin by offering our views regarding the important subject of this hearing: "The growing problem of identity theft and its relationship to the Fair Credit Reporting Act". I will summarize some important research that we have conducted which has guided AARP's thinking about these important issues. I have attached as appendices to my written remarks the results of two key studies that underpin today's testimony.[1]

Identity theft is the co-opting of names, Social Security numbers, credit card numbers, or other pieces of personal information for fraudulent purposes. The fraud most often perpetrated takes the form of using someone else's account

[1] See attached: "Identity Theft: Experience of Older Complainants", and "The Fair Credit Reporting Act: Issues and Policy Options".

identity for purposes of financial theft. It can also take the form of an impostor – that is, someone assuming another person's identity in order to seek payment under false pretenses for provision of professional or other services - and to avoid accurate identification or detection.

Identity theft occurs when an individual's personal identifying information (for example, name, Social Security number, date of birth, or mother's maiden name) is stolen by another person and used to commit fraud or engage in other unlawful activities. Often, this stolen information is used to establish credit, run up debt, or take over existing financial accounts. Typically, identity theft damages the victim's credit, making it difficult for the victim to buy a home or car, rent an apartment, obtain employment, or purchase insurance.

Victims often spend substantial amounts of time and money resolving problems created by identity theft. Common problems include the victim's having to contact credit bureaus repeatedly in an attempt to clear his or her credit reports of fraudulent accounts, being turned down for credit based on the incorrect information contained in the victim's credit report, and receiving calls from creditors seeking to collect on the fraudulent accounts.

I mentioned two studies. The first study confirms the seriousness of the identity theft problem for older persons. With a membership of over 35 million persons, AARP views with alarm the risk that identity theft poses to the personal security of

all Americans, young and old, well educated or not. However, our research does indicate a greater vulnerability of older Americans, based on the higher proportion of those age 50 years and older who report being victimized by identity theft, compared to the proportion of all age groups making such reports.

The second study represents an extensive review of the research literature on the Fair Credit Reporting Act. This AARP report describes the range of risks faced by consumers that result from erroneous information (elements) -- some resulting from identity theft. A variety of policy options for reform of FCRA emerged from this examination.

We should recognize that all Americans are vulnerable to the fraudulent use of their – or someone else's - personal information. After all, we are known as the information society. But mid-life and older Americans are particularly vulnerable targets for this type of criminal activity because they control a proportionately larger share of the nation's financial assets, and because there are likely to be more access points to a longer personal history that can be tapped into and exploited. For those near or in retirement, the costs of identity theft under any guise are particularly high, bringing a sense of violation and a loss of individual security that cannot easily be recovered.

The magnitude of the nation's problem with identity theft is just now coming to light. Identity theft has been listed by the U.S. Federal Trade Commission (FTC) as the fastest growing form of crime in the nation. Depending on the reporting source and the manner in which the information was collected, the estimates range from 500,000 to 1.1 million victims for the year 2001 alone. Even the lower estimate seems staggering.

Estimates also vary as to the financial losses incurred, and the time and effort it takes to reestablish a victim's proper credit and community standing. For example, according to studies done by the FTC and by the Privacy Rights Clearinghouse, the average victim spends about 175 hours and $1,100 in out-of-pocket expenses. Once victimized, an individual may never completely recover his or her "good name". The risk of being victimized has been amplified through the availability and use of today's high-tech information resources and tools.

The Identity Theft and Assumption Deterrence Act of 1998 – known by short-hand as the Identity Theft Act – made it a federal crime to knowingly transfer or use a means of identification of another person with the intent to commit, aid or abet any unlawful activity under federal law, or any activity that represents a felony under state or local law. Most states have passed similar laws related to identity theft – that is, most state laws make identity theft a criminal offense.

Thousands of impostors have been caught and prosecuted, most often by the U.S. Postal Service Inspection Service (which investigates mail fraud) and the U.S. Secret Service's financial crime division. Also important are the efforts of efforts of state and local law enforcement agencies – although all law enforcement resources are being heavily taxed by homeland security and anti-terrorism responsibilities. Notwithstanding these efforts, it appears that identity theft remains a high-profit, low-risk and -- until recently at least -- a low-penalty crime.

Identity Theft: The Experience of Older Complainants

The Identity Theft and Assumption Deterrence Act of 1998 made the actual theft of an individual's identifying information a specific federal crime, and authorized the creation of the FTC's Identity Theft Data Clearinghouse and database -- which has been in existence since 1999.

The complaint data are based on self-reporting by the complainant either to the FTC or to another agency that subsequently forwarded the complaint to the FTC.[2] Since inception of the database, the FTC has reported major increases in the number of telephone calls from consumers to its Clearinghouse hotline. Calls from consumers increased from an average of 445 calls per week in the first month the hotline was in operation (November 1999), to an average of 3,000 calls per week in December

[2] The question may arise regarding how to appropriately interpret consumer complaints data. We take the perspective that consumer complaints can serve as an early-warning function leading to increased accountability and safer, more effective, high quality processes, products and services.

2001. In addition to the toll-free hotline, consumers can file a complaint online or by mail.

In order to get a sense of the vulnerability among those 50 and older to identity theft, AARP requested that the FTC prepare two sets of tabulations based on complaint data gathered through the Identity Theft Data Clearinghouse for the year 2001. The 2001 data report on 86,168 identity theft complainants, with 72 percent of these (61,956 complainants) reporting age information.

For the year 2001, more than three-quarters (78%) of complainants who reported their age (n=61,956) were under 50 years old, while 22 percent of complainants were 50 years of age or older. We then asked the FTC to group its data for complainants on identity theft crimes, for those that provided their ages, into their classification system for different types of fraud.

Key Results:

Credit Card Fraud: Among the general types of fraud identified by the FTC, forty-two percent of all complainants reported having their stolen information used in an effort to commit credit card fraud. Of complainants reporting this type of fraud, 62 percent reported that their information was used in an attempt to establish new credit, while 24 percent reported their information was used in an effort to access

existing credit accounts. Half (51%) of complainants age 50 and older reported having their stolen information used in an attempt to commit credit card fraud. Of complainants reporting attempts at this type of fraud, two-thirds (66%) reported their information had been used in an effort to establish new credit, while one-third (33%) reported their information was used in an attempt to access existing credit accounts.

Telephone or Utilities Fraud: Twenty percent of all complainants reported having their stolen information used in an effort to commit telephone and utilities fraud. Nearly half (48%) of complainants experiencing this type attempt at fraud reported their information had been used in an effort to establish new wireless telephone service. Seventeen percent of complainants age 50 and older reported having their stolen information used in an effort to commit telephone and utilities fraud. Almost two-thirds (64%) of complainants in this age group experiencing this type of attempt at fraud reported their information had been used in an effort to establish new wireless telephone service.

Bank Fraud: Thirteen percent of all complainants reported having their stolen information used in an effort to commit bank fraud. Nearly half (47%) of complainants experiencing this type of attempted fraud reported their information had been used in an effort to commit check fraud. Eleven percent of complainants age 50 and older reported having their stolen information used in an effort to

commit bank fraud. Sixty-three percent of older complainants experiencing this type of attempt at fraud reported their information had been used in an effort to commit check fraud.

Loan Fraud: Six percent of all complainants reported having their stolen information used in an effort to commit loan fraud. Half (53%) of complainants experiencing this type of attempted fraud reported their information had been used in an effort to secure a personal or business loan. Seven percent of complainants age 50 and older reported having their stolen information used in an effort to commit loan fraud. Of complainants experiencing this type of attempt at loan fraud, 56 percent reported their information had been used in an effort to secure a personal or business loan.

Overall, ten percent of all complainants that reported their personal information had been stolen indicated that it was used in an attempt to commit some type of fraud. However, nearly double that proportion, eighteen percent of complainants age 50 and older, reported attempted identity theft fraud. We believe that further collection and analysis of complaint data are necessary to better understand the nature of identity theft crimes and to devise more effective prevention and enforcement policies.

Implications for the Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA), enacted in 1970, is the foundation of our national credit system. Consumer reporting agencies (CRAs) collect and compile information on consumers' creditworthiness from financial institutions, public records, and other sources. FCRA applies to the personal credit records maintained by CRAs. The FCRA also outlines a consumer's rights in relation to his or her credit report, as well as permissible uses for credit reports and disclosure requirements. In 1996, the FCRA was amended and now contains seven specific federal preemptions (due to sunset on January 1, 2004, unless Congress extends them) that prevent states from overriding or changing:

- The responsibilities of organizations and businesses that furnish information to reporting agencies;
- The duties of organizations and businesses to notify consumers when they have been denied credit or employment based on information in their credit reports;
- Procedures that a consumer reporting agency must use if a consumer disputes the accuracy of information;
- The information that may be included in consumer reports, including the time during which consumer reporting agencies are permitted to report adverse data;

- The form or content of the summary of rights that a consumer reporting agency is required to provide to a consumer along with information in the consumer's file;
- The exchange of information among affiliated institutions; and
- Prescreening procedures that provide consumers with credit or other financial services or product lines.

The consumer credit reporting industry is a $6 billion industry that provides information about consumers to a wide variety of businesses. Information on consumers is purchased by lenders, credit sellers, insurance companies and landlords, and by employers seeking information on prospective or current employees. The largest sources of credit reports are the three national consumer reporting agencies (CRAs) that collectively maintain an estimated 570 million files on U.S. consumers. Each CRA collects its own data on an individual consumer and maintains its own file on that consumer. It should come as no surprise that the credit reporting industry is the most extensive user of consumer data in the private sector.

In addition to selling credit reports, CRAs sell prescreened lists of consumers to providers of credit and insurance products. Prescreening involves CRAs' creating a list of consumers who meet criteria specified by purchasers of the list. For example,

credit card companies use prescreened lists to identify and solicit consumers who qualify for "pre-approved" offers of their credit card product.

As a result of the large amounts of data involved, the credit reporting industry relies heavily on computer automation, and information is transferred, sorted, stored, and retrieved electronically. To facilitate this automation, many creditors and other furnishers of information to CRAs use a standardized computer program to report data to CRAs. Information provided to CRAs is usually received monthly and downloaded into their databases.

The widespread use of credit reports for an increasing variety of purposes, and the large amount of information processed by CRAs, raise a number of issues regarding the FCRA's uses and effects. One of the major goals of the FCRA is to promote accuracy in credit reporting by requiring CRAs to use reasonable procedures. Despite FCRA protections, available data suggest that assuring the accuracy of the information in credit reports continues to be a concern. Incorrect information has too often been included in consumer credit reports.[3]

[3] A 2000 study examining consumer credit reports found that over half of the credit reports examined contained errors. A 1998 study found that 70 percent of credit reports investigated contained incorrect information. Of these reports, 29 percent contained errors significant enough to have serious adverse consequences for the consumer's credit, and 41 percent contained personal identifying information that was either incorrect or obsolete. See Appendix 2.

Another accuracy issue is that information creditors provide to CRAs may be incomplete and positive information may be missing. The FCRA does not require creditors to report account payment information to any CRA. Rather, creditors are free to report to none, one, two, or all three of the national CRAs.

Additionally, some companies apparently intentionally withhold positive credit information to prevent the loss of customers to competitors. As a result, the credit reports of these consumers will not reflect positive payment history, and the consumer will be unable to access less costly products and services.

Inaccuracies can also occur when a creditor sells a delinquent account to a debt collector. Once the original creditor sells the account to a debt collector, the debt collector becomes the furnisher of information on this account to the CRAs. The main source of inaccuracy in this case results from incorrect reporting of the date of initial delinquency on the account.[4]

A further source of inaccurate information is error in the electronic merging of files that occurs when one consumer's credit information is mixed with another

[4] One concern is that debt collectors may report the date they purchased or received the account as the date of initial delinquency, even though the actual date of initial delinquency was likely much earlier. Because the FCRA stipulates that most negative information remains on a consumer credit report for seven years from the date of initial delinquency, establishing this date is important to consumers attempting to restore their credit.

consumer's file. This typically occurs with consumers who have similar identifying information such as a similar name or Social Security number.

Yet another source of inaccuracy occurs when CRA subscribers request information on one consumer from a CRA database, and obtain data on another consumer instead. This problem occurs because the accuracy of the information received from a CRA is inversely related to the specificity of the identifying data elements that are used to search the database. That is, subscribers who use fewer identifying elements are more likely to receive credit information unrelated to the consumer about whom they are seeking credit information. For example, a subscriber who uses only name and address information will likely receive more matches (and consequently less accurate information) than a subscriber who uses additional identifiers (such as Social Security number and date of birth).

Consumers are typically required to pay a fee when obtaining a copy of their credit report. The FCRA allows CRAs to charge consumers a fee of up to $9 (plus applicable state tax) for a copy of their credit report. Six states entitle consumers to one free credit report from each CRA annually, while other states cap the cost of credit reports below the federally mandated level.

Because most consumers have separate files at all three national CRAs, consumers are well-advised to purchase their credit report from all of them to ensure that each

of their credit reports are accurate. They are used by potential lenders to provide an instant summary of information contained in the consumer's credit report and may be used to rank consumers to determine whether they qualify for a loan, how much they should be lent, and at what rate.

Then there is the problem of identity theft that I raised earlier. At issue here is the role of the FCRA in preventing identity theft and assisting victims of this crime. Previously I noted that older persons can be an appealing target for such theft because they typically have significant available credit to draw on. They can also be victimized by family members or caregivers who have access to their personal information. It appears that all too often, the identity thief takes the individual's personal information and uses it to open fraudulent accounts based on the unknowing victim's credit report information.

FTC complaint data show that consumers often experience substantial difficulty in correcting information they dispute. One concern is that reinvestigation procedures used by CRAs are inadequate. Another problem is the reappearance of incorrect information previously deleted from a consumer's credit report. In addition, victims of identity theft have reported difficulty in removing fraudulent items from their credit reports even after the identity theft has been discovered.

Another FCRA issue involves the preemption of some aspects of existing state credit reporting laws. Most states have laws relating to credit reporting, and generally the FCRA does not preempt state laws that provide greater consumer protections. Should the state preemptions expire on January 1, 2004, as required under the FCRA, states would be allowed to enact legislation governing the sharing of such information.

Our survey of issues concludes with the two-year statute of limitations provided by the FCRA. This issue is the result of a 2001 Supreme Court decision involving an identity theft victim's suit against a CRA for failing to take reasonable steps to ensure the CRA was issuing a credit report for the right person. The court's ruling is a major concern for identity theft victims and their counsels because it takes an average of 14 months for victims to learn of the theft and subsequent damage to their credit reports. As a result, consumers who do not learn of problems in their credit reports quickly enough may have no legal recourse.

Some Recommendations

To address these concerns, we recommend that Congress and the Administration:

- Provide stronger enforcement of rules requiring the date of initial delinquency to be reported correctly by debt collectors. The FCRA requires furnishers of

such information to verify the accuracy of the data reported when challenged by a consumer. This proposal is intended to prevent the reporting of negative information beyond the time limits provided by the FCRA.

- Require subscribers who purchase credit reports from CRAs to provide the same standard of identification to retrieve a consumer's credit report as is required of consumers seeking their own credit report. Because CRAs have procedures in place for consumer access, these same procedures can be applied to subscribers requesting credit reports.

- Require CRAs to provide consumers with at least one annual free credit report a year to make it easier and less expensive for consumers to monitor their credit reports. Prohibitions need to be enacted that protect consumers from fraudulent "credit-repair" practitioners.

- Allow consumers to place a security freeze on their credit report, and issue to consumers a password to prevent their credit report from being accessed without their express authorization. California recently enacted such a provision. This procedure slows down the process for retrieving a consumer's credit report because the consumer must first contact the CRAs and give permission for the release of his or her credit report to the specified individual or business, thereby providing an extra check to prevent fraud.

- Require CRAs to permanently block fraudulent accounts on the credit reports of identity theft victims. Such blocking is required under California law and has been proposed under federal legislation. This requires CRAs to correctly identify that the account is fraudulent despite the fact that the account may have been sold to a debt collector and been reported as a separate account.

- Require the FTC to monitor how effectively consumer disputes with CRAs are resolved.

- Allow the Federal preemptions to expire as originally intended under the FCRA unless federal legislation providing greater consumer protections can be enacted.

- Change the statute of limitations to allow consumers more time to discover potential problems in their credit reports. Federal legislation has been proposed to extend the statute of limitations. Changing it to two years from the time the violation is discovered, or should have been discovered by the exercise of due diligence by the consumer, would give consumers a longer time frame in which to act.

Closing Thoughts

AARP supports strengthened federal, state and local efforts to hold the perpetrators of identity theft and fraud accountable. We are prepared to work with you Chairman Shelby, Senator Sarbanes, and with the other Members of this Committee in this regard. However, we also believe that efforts to improve accountability should be complemented with effective measures to provide victim assistance.

And we believe that the practices of credit-reporting agencies should be reformed to protect consumers and businesses against erroneous information, provide greater consumer access to credit files, enable consumers to correct erroneous information more easily, require that credit reports be more user-friendly and require the purging of files after a reasonable time. We would so be happy to work with the Committee in updating and upgrading the FCRA.

I would be pleased to answer any questions that you may have.