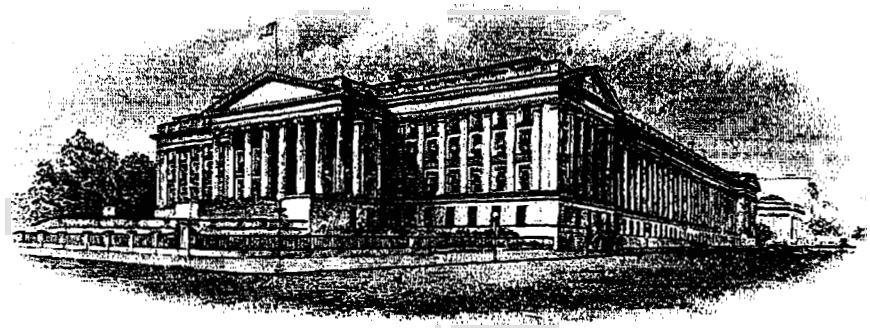

DEPARTMENT OF THE TREASURY
OFFICE OF PUBLIC AFFAIRS

Embargoed Until 10:00 am EDT
May 8, 2003

Contact: **Betsy Holahan**
202-622-2960

Testimony of
Wayne A. Abernathy
Assistant Secretary for Financial Institutions
U.S. Department of the Treasury
before the
Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
U.S. House of Representatives

Good morning Chairman Bachus, Ranking Member Sanders, and members of the subcommittee. It is an honor to appear before you today. There could hardly be a more important subject to consider than the information infrastructure of our financial system. So much of the economy, and the welfare of every participant in the economy, is dependent on getting the legal structure of that system right.

In 1996, the Congress undertook an experiment, to determine whether uniform national standards for financial information sharing was the right approach. These uniform standards were embodied in the provisions of the Fair Credit Reporting Act (FCRA). Those provisions are scheduled to sunset at the end of this year. It is therefore appropriate now that Congress evaluate the results of that experiment. We are eager to participate in that evaluation as we develop Administration policy.

To begin with, since the FCRA experience with uniform national standards began, we have witnessed significant increases in the availability of credit to Americans. It is the impact of the legislation on Americans—consumers and businesses—that should guide us in our considerations. We should keep in mind that all Americans have two interests at stake in this matter: an interest in access to credit and other financial services, and an interest in the security of their personal financial information. As Congress reviews these uniform standards, these two interests need to be weighed and taken together and accommodated. I believe that they can be.

In this evaluation, we would suggest considering the following questions:

- Do uniform national standards facilitate or harm the fight against identity theft? Can greater progress against the crime be made with or without uniform national standards for information sharing?
- Do uniform national standards strengthen or undermine the security of personal financial information?
- Do uniform national standards reduce or increase the costs to consumers of financial services?
- Do uniform national standards bring more or fewer people into the mainstream of financial services?
- To what extent do uniform national standards lead to an increase or decrease in the variety of financial services offered to consumers?
- To what extent do uniform national standards help or hinder job creation?
- Is small business development helped or harmed by uniform national standards?
- What would be the impact on unwanted customer solicitations if the uniform standards expired? To what extent are such solicitations facilitated by uniform national standards?
- In short, what costs or benefits to the economy as a whole can be attributed to uniform national standards for information sharing, and what would be the economic impact if they were allowed to expire?

Undoubtedly, there are other questions that should be examined.

At Treasury, one area that we have been particularly concerned about is the role that FCRA uniform national standards play in the fight against identity theft. The importance of this concern can be understood by a brief review of the nature of the crime.

Identity theft is one of the fastest growing crimes in America. By some estimates, there will be as many as one million new victims this year, with many times that number already in the ranks of sufferers.

In a recent national survey of homeowners, 12% reported having been casualties of identity theft, and 22% reported knowing family, friends, or acquaintances who have been. It is hard to think of another crime that has touched such a large portion of Americans. In that same survey, 90% said that they were concerned that they might be a target of identity theft. A separate survey recently found that Americans are more concerned about becoming a victim of identity theft than they are of losing their job. No wonder that 83% believe that the government should take steps to fight the crime.

Many suffer from the unauthorized use of their own legitimate credit card. This is one of the milder versions of the crime, and today perhaps the most common. Fortunately, it is also an aspect where great progress has been achieved in fighting it. As long as the consumer is diligent and promptly reports lost or stolen cards or unauthorized charges, the direct liability to the card holder is zero. The Truth in Lending Act sets the maximum loss at $50, but credit card companies have found that there are great benefits in consumer confidence from eliminating all

liability for the innocent victim. The loss still occurs, though, and it adds up to billions each year, ultimately born by all card users in higher prices and higher interest rates.

Credit card companies also have elaborate and well-designed information-sharing systems in place, neuronetworks, that monitor customers' accounts and quickly notify them of charges that are out of the ordinary, such as purchases outside the customers' normal buying patterns or far from home. This is an important deterrent to this type of identity theft. Other financial sectors are working on deterrents appropriate for their business. Much more needs to be done.

The crime occurs in great variety. As I speak, somewhere, someone is using someone else's good name to engage in fraud, to steal from a furniture store, rob a bank account, engage in stock swindles, write bad checks, run up huge phone bills, escape gambling debts, shield illegal drug deals, create false résumés, impersonate doctors or other professionals, destroy reputations.

Do not look for patriotism among identity thieves. When our soldiers, sailors, and airmen move to the front lines to engage the enemy, the identity thieves are ready to take advantage of their absence to steal their identities to commit fraud. I would guess that the soldier in the Third Infantry Division in Baghdad is not giving much thought to his bank account, or worrying about his credit cards, certainly not looking at his financial statements. But the fraudster is paying attention, for he knows that the fraud could go undetected for a long time, unless friends and family are vigilant, on the watch here at home over the financial affairs of the service man and woman overseas.

Not even the dead are immune from identity theft. Necrolarceny is one of the more repulsive, but not uncommon, faces of the crime. Thieves scan the obituaries and gather the information provided there to impersonate the deceased. From the obituary, the thief harvests a wealth of knowledge: the full name, a maiden name, age, names of family members, possibly education and charitable activities—all types of information that the thief can draw from to impersonate the deceased and, possibly, other family members. And closing down financial accounts is not usually high on the To Do List of bereaved family members. Yet there may be a tragic surprise awaiting when a will reaches probate and the family members learn how financially active their mother was in the days and weeks following her death.

No one sitting in this hearing room is immune from identity theft. Undoubtedly, there are many here who have been victimized or know someone who has. There may be some here who are being victimized right now and won't know of it for several more weeks or months.

Perhaps someone is dumpster diving, going through your trash to get important bits of information about you or your accounts. Perhaps someone will call, impersonating a government employee, asking to "verify" some of your personal data in order to continue to send you your Social Security check or veterans benefits. Maybe you will be snared by a supposedly "free" service on the Internet, that only needs your name, address, date of birth, and so on, in order to provide you with access to the free service.

Arguably, the most virulent form of identity theft occurs where the crook takes your good name and uses it to open new accounts that you know nothing of, with the statements going to places

you have never been, so that weeks and months pass without your knowledge of the fraud. The crook may even keep up minimum payments for a time until he can max out on the credit limits. Then he disappears, the payments stop and the creditors come looking. But they don't find the crook. They don't look for the crook. They look for you. And you discover the fraud when you can't pay for your dinner because your charge will not clear. Your home equity loan is turned down because there already is a lien on your house. You lose your job, because, though your boss is very sorry and thought you were an exemplary employee, he can't have someone in such a sensitive job who has such a poor credit history.

And then you will see perhaps the most painful face of all the many faces associated with the crime of identity theft, the face of the victim. Where do you go? How do you begin to clear your name? How do you convince creditors all around the country that you never made those transactions, that there must be some mistake? Do you turn to your local police department? They might fill out a police report, but victims report that many do not. What can the local police do about it anyway? The crime took place in Bigtown, not in your home town. Will the Bigtown police take up the case? Maybe, but you live in Virginia. Who will handle a case for a victim living in Charlottesville, for fraudulent transactions made in Miami, Denver, and San Francisco, with money borrowed over the Internet from a bank headquartered in Philadelphia? Crooks have long sought to exploit State lines to avoid punishment.

The General Accounting Office reports that it can take victims as many as 175 man hours to clear their name and their records. That would be the equivalent of more than one full month of 8-hour days, five-day work weeks of full-time work. Of course, that is spread out over time, over months and sometimes years, with thousands of dollars of expenses.

What role have the uniform national standards in the FCRA played in the fight against identity theft? What role might they play? Are they more likely to cause the crime, or can they be enlisted in the fight against it?

The answer lies in information. Information is what the FCRA is all about. So, first of all, we need to consider the role of information in identity theft. Certainly the crook uses information. He uses information to craft a mask, as much in the likeness of his victim as he can make it. What steps can we take, if any, to deny the thief the information tools he needs to make his mask? In answering that question, what tools can we find to fight the crime?

But does it end there? In what way might we be able to put information to work to fight the crime? If the merchant or banker knows more about his customer than the thief does, can we unmask the crook and prevent a loss from occurring? If information about the thief can cross state lines faster than he can, might we enable the sheriff to meet the thief at his next stop?

And what role does information play in restoring the records of victims? Are uniform standards contributing to placing bad information on consumer records? Can they be harnessed in the effort to eradicate the false information?

As we consider the uniform standards for information sharing under the FCRA, we anticipate working with you to consider how this review can help in the crucial fight against identity theft.

So, as I said in the beginning, whether considered from the impact on each family in America, or on the economy as a whole, there could hardly be a more important inquiry than the one you begin today. We are eager to join with you in that review. It is vitally important that we get the answer right.

Thank you. I will now be pleased to answer your questions.