TESTIMONY OF

JAMES K. KALLSTROM
SENIOR EXECUTIVE VICE PRESIDENT
MBNA AMERICA BANK, N.A.

BEFORE THE

FINANCIAL INSTITUTIONS SUBCOMMITTEE
COMMITTEE ON FINANCIAL SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON

FIGHTING IDENTITY THEFT

2128 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, D.C.
JUNE 24, 2003

INTRODUCTION

Thank you Mr. Chairman for inviting me here today. I think I can safely speak for the entire industry in complimenting the committee for the thoroughness with which you are examining the issues relating to reauthorizing the Fair Credit Reporting Act. From our perspective, you have constructed a compelling record from which to legislate and we have high praise for the diligence and dedication of the staff who have brought all of this together.

Regarding identity theft, we are in complete agreement with you and the other members. Identity theft – like other serious crimes - is an attack on our citizens, our businesses, and on our economy. It accounts for only about four percent of the fraud we experience but, as you have just heard, it often exacts a personal cost of time, reputation and frustration that is very hard to measure.

I have years of experience dealing with the crime of identity theft and, unquestionably, more, much more, can and should be done in each of four aspects - - prevention, detection, enforcement and victim assistance.

The issues relating to identity theft are very often quite complex. They run the gamut from the common phenomenon of theft by a family member, friend or associate to how we can more quickly restore the good name and credit reputations of unwitting victims. Viable solutions likely will involve greater participation by all of us - - the credit granting industry, retailers, the credit bureaus, law enforcement, prosecutors, government agencies, and consumers.

No one disputes that identity theft is a serious crime that should be attacked vigorously. It also is a crime that victimizes consumers and industry alike. And as with many crimes, the cliché "forewarned is forearmed" applies. Insuring the availability of and arming both businesses and potential victims alike with key information goes a long way toward prevention and apprehension. As Assistant Secretary Abernathy remarked recently, "Identity theft is not caused by information. It is caused by a *lack* of information."

SUMMARY

In summarizing my statement for the record, I would like to make four points.

First, the interests of our customers and the interests of industry are synonymous here. Our business philosophy is "find the right customers and keep them." We want our customers to be able to use our products – and use them securely. We want our customers to have confidence that we will help protect them against the scourge of identity theft.

When fraud does occur, our customers are not responsible for the fraudulent charges and we provide assistance both to help stop further damage and to help in recovering from the identity theft. But, as we have just heard, it is far more difficult to restore the confidence of victims and to relieve the effects of having their identities stolen. We agree with our customers who say, reputations, goodwill, financial well being and consumer confidence are all put at risk because of identity theft. In the end, it hurts everyone.

Second, prevention and detection of identity theft is what we do with every application and every transaction seven days a week, 365 days a year. We invest millions of dollars preventing and detecting identity theft and other types of fraud. We employ hundreds of people who specialize in fraud detection and prevention and have a sizable cadre of people dedicated to ensuring our customers are properly identified. We employ extremely sophisticated neural-networks and experience-based automated strategies to find and reduce fraud and identity theft. From exploring discrepancies between applications and credit reports to scrutinizing hundreds of thousands of daily transactions for anomalies, we fight identity theft from the credit application stage through loan repayment.

Our customers are critical participants in the process but there is no question that the Fair Credit Reporting Act is the foundation of this effort. To be successful, we rely upon the kind of uniform, current credit information that the FCRA has given us.

The third point I would like to make is setting the record straight on a couple things: affiliate sharing and prescreening. With affiliate sharing we are aware of no instance - not one - where affiliate sharing resulted in identity theft. To the contrary, it helps the industry fight identity theft.

Our experience with prescreening is similar: prescreening results in substantially fewer fraud attempts – not more. A study released last week by the Information Policy Institute (IPI), a copy of which I am submitting with my statement for the record, confirms that the same holds true for the entire industry. In fact, the study found that the industry losses from fraudulent prescreened applications amount to four one thousandths of one percent of total sales volume and eliminating prescreening would likely result in an <u>increase</u> in identity theft. That is so because prescreened offers reflect only names and addresses, less than is in a telephone book, and the prescreening process involves <u>more</u> filtering not less.

One final point: Assistant Secretary of the Treasury Wayne Abernathy understands the industry, understands the problem, and he and others at Treasury have talked about the need for a comprehensive approach to address the problem of identity theft. We agree that any approach should include enhanced prevention, detection and victim assistance. It should include reauthorizing FCRA because, as Assistant Secretary Abernathy says, to do otherwise risks “creating shadows,” where identity theft can occur. On the enforcement side, the solution should include stiffer penalties reflecting the serious and pervasive nature of this crime.

We also agree that any solution should help consumers make more informed decisions about information sharing. This can happen by making privacy notices shorter, simpler and in plain English and making opt out procedures easier and uniform so that consumers can more easily exercise control of personal information and in a more meaningful way.

Everyone agrees that it would be of enormous benefit to provide consumers with easily digestible privacy notices that include easy opt out procedures. In fact, in a recent survey we found that our customers overwhelmingly support a simple, food label-like notice as the kind of notice they want – a notice they will actually read, that is easily comprehensible, and which allows busy people an opportunity to participate in information sharing decisions in a more meaningful way. It is simply a good idea that will be of great benefit to consumers.

In the end, legislating more and better tools for law enforcement, consumers and the industry to use to prevent, detect and recover from identity theft is a consumer issue that will help us all. We applaud your attention to these critical issues and I look forward to your questions.

HOW MBNA PREVENTS & DETECTS IDENTITY THEFT

MBNA proactively contains fraud by reviewing new applications for discrepancies when compared to credit reports and other available data, and by continuously evaluating Customer-initiated sales transactions and requests for credit. These controls can be grouped into three categories: the prevention of new account fraud, the prevention of fraud on existing accounts, and the detection of fraud on existing accounts.

A. New Account Fraud Prevention

In today's national credit market, all credit issuers are more vulnerable to fraudulent requests for credit due to the non face-to-face nature of the process. As in all key decision-making functions, MBNA emphasizes human judgment.

Identity verification begins immediately after a new application is received and entered into the system. The system compares data provided on the credit application to data returned from a credit-reporting agency but a real person reviews this information. In addition to credit report data, other tools used to assist hundreds of analysts in identifying discrepancies and suspicious activity include:

- experience-based strategies that identify potential anomalies
- a fraud scoring model
- consumer statements
- security alerts, and
- an internal fraud database

Moreover, our fraud analysts apply their experience and judgment to identify suspicious applications.

If the application is judged suspicious, analysts have available a variety of tools to verify information and, in many cases, are able to locate the actual applicant to verify the validity of the application by speaking with this person on the telephone. If fraud is identified, victims are instructed to contact each credit reporting agency to place a statement on their credit file to let other credit grantors know that they have been victimized. Additionally, victims are given a toll-free number to the Federal Trade

Commission (FTC) to obtain information about identity theft and to add their name to the FTC fraud database.

In addition, credit card issuers are required to report confirmed identity theft to an external fraud database known as Issuers Clearinghouse Service ("ICS"). ICS is jointly owned by MasterCard and Visa. The service provides notifications to credit card grantors about fraudulent or potentially fraudulent activity involving consumers' personal information. As a secondary precaution, we use ICS to review and compare new accounts to the ICS database to ensure that any suspicious activity is identified and investigated.

B. Existing Account Fraud Prevention - Authorizations

MBNA employs state-of-the-art authorization systems to prevent fraud. A variety of sophisticated statistical techniques allow the vast majority of our Customers to use their cards without interruption, while also identifying transactions that present a high degree of fraud risk. Since 2001, MBNA has received seven awards from MasterCard and Visa for the performance of this authorization system.

Empirically derived strategies are developed based on historical portfolio performance. Central to the strategies is the use of a customized fraud score that employs neural network modeling techniques to make decisions and learn from changing patterns of fraudulent activity.

Use of this technology has allowed MBNA to maintain industry-leading authorization approval rates. However, in order to mitigate fraud risk we still decline or ask a merchant to contact us on over 2 million transactions annually. Merchants who call in response to a referral request are routed to an analyst who validates that the person presenting the card is our Customer. Referral calls are always answered immediately and are handled 24 hours a day, seven days a week.

C. Existing Account Fraud Detection

Authorization strategies alone cannot contain fraudulent activity. MBNA employs hundreds of fraud analysts who evaluate unusual spending patterns and contact Customers to determine if they believe fraud is occurring on their account. The same statistical techniques and tools used to establish authorization strategies are used to develop and employ fraud detection strategies.

For example, MBNA requires all Customers to contact us to activate new cards. A similar approach is taken when requests for change of address or requests for access devices (cards, check, ACH, etc.) are made. At this stage, specialized MBNA people apply strategies specifically designed to prevent and detect unauthorized access to a Customer's account.

When a fraud claim is received, MBNA conducts investigation. When the fraud claim is accepted, the Customer is absolved of any financial responsibility resulting from the fraud and their credit bureau report is appropriately corrected. A fraud specialist will work with the Customer to discuss the appropriate steps that should be taken to protect themselves against future crimes and an identity theft brochure, which we created, is mailed that explains the process.

We will continue to investigate cases by filing a Suspicious Activity Report ("SAR") on appropriate accounts in accordance with Bank Secrecy Act guidelines. Moreover, we employ fraud investigators, former law enforcement officers that work with federal, state and local law enforcement agencies on identifying and prosecuting fraud perpetrators.

An important factor in minimizing fraud losses is the ability to review transactions quickly and thoroughly. Continuous investments in the fraud detection systems have created greater efficiencies and better methods for isolating the riskiest transactions and accounts. Isolating and prioritizing the fraud more efficiently lets us find the fraud sooner. Finding the fraud sooner contains the loss. For example, the following is an excerpt from a letter received from a Customer who recently experienced identity theft:

> *" We had a stranger trying to move our account to X in the quest to use our credit. You were able to catch this attempted identity theft early and inform us of all the proper avenues to pursue to keep our financial information safe. We applaud you. Your company consistently calls us with any suspicious activity or charge, which is very reassuring."*

Recent improvements have allowed MBNA to reduce the average balance for a fraud claim to less than 2001 levels. As a result, MBNA has been able to reduce fraud losses even with a growing loan portfolio.

HELP IS NEEDED TO COMBAT IDENTITY THEFT

We have a number of specific suggestions but in general, our experience convinces us that six categories need to be enhanced. They are:

- Greater national uniformity, not only with FCRA, but in most aspects of combating identity theft - lack of uniformity directly benefits identity thieves.
- Increased penalties, and increased resources for law enforcement training, investigation and prosecution of identity theft – the duties of law enforcement at all levels have grown tremendously in recent years – if we are serious about combating this particular crime, training and resources must be dedicated to it.
- Greater consumer participation through increased access and simplifying the notice and choice process – make information accessible, comprehensible, and make consumer choice informed and easy.

- Consistent with what Assistant Secretary Abernathy said last week, greater information sharing within the industry, especially along the lines of what The Consumer Data Industry Association (CDIA) recently announced about sharing of fraud alerts between the credit bureaus, and;
- Greater victim assistance once the crime has been established.

Specifically, we offer the following suggestions as well:

Training and Resources for State and Local law enforcement

Most identity theft investigations fall to local authorities. We applaud what Secret Service is doing to provide state-of-the-art training and think more should be done. Local law enforcement at the "first responders" need more training and resources given the rate of growth of this crime.

Standardized Reporting/Common Definitions

Because identity theft investigations are frequently multi-jurisdictional, a lack of common definitions and standardized reporting, particularly at the local level, is a significant problem that often results in cases not being investigated.

Increased Penalties

Many identity theft instances are not investigated because, even if proven, prosecutors will not expend scarce resources to prosecute because of the minor nature of the crime. Increasing the penalties substantially likely would raise both the number of prosecutions and the deterrence value.

Credit Card Number Truncation

The recent policy change to mandating truncation on all electronically printed receipts to include expiration date is strongly supported across the industry.

Nationwide Service of Process

The Patriot Act contains authorization for nationwide service of process when certain computer related electronic evidence is being sought. This was done because of the interstate nature of most investigations seeking electronic evidence. The same is true for identity theft. Frequently the victim and perpetrator are in different jurisdictions.

Centralized Data Base

Currently there is no central database accessible to both law enforcement and industry reflecting known fraudulent names, addresses, account numbers, etc.

Law Enforcement Coordinating Council

S. 1742 in the 107th Congress contained provisions to have a coordinating body for law enforcement on this issue. The more commonality there is between jurisdictions, the more it helps the industry deal with what is often a multi-jurisdiction issue.

Civil Restitution/Civil Forfeiture

Although the amounts may be small, forfeiture provisions that inure to the financial benefit of local law enforcement and create liability to the victims for actual damages could increase the cost to identity thieves and help victims recover what they have to pay out-of-pocket.

CONCLUSION

We agree with the approach taken by Assistant Secretary of the Treasury Abernathy - to be of maximum effectiveness, any approach to reducing identity theft should be comprehensive to better serve consumers, the government, the private sector, and, ultimately, the national economy.

The reauthorization of the seven preemptions added to FCRA in 1996 is a necessary starting point. As Assistant Secretary Abernathy says, to do otherwise risks creating shadows where identity theft can flourish. This is so because the FCRA, as amended, has provided a nationwide financial infrastructure that enables businesses to obtain immediate and reliable credit information on which to base key financial decisions but also to use in properly identifying customers and ferreting out identity thieves. And we should not forget, it has provided a mechanism that consumers rely upon every minute of every day to better their lives, and to aid in protecting themselves.

Finally, while we are investing millions in fraud detection and prevention strategies, and in people to assist our customers and maintain their confidence, we agree that more must be done across the industry, across the government and even by consumers if, collectively, we are to be successful.