Statement of Robert Ryan,

Senior Director of Government Relations
TransUnion, LLC

Before the

Subcommittee on Crime, Terrorism and Homeland Security
Of the Judiciary Committee

HR 1731: The Identity Theft Penalty Enhancement Act
&
HR 3693: Identity Theft Investigations and Prosecution Act of 2003

March 23, 2004

Introduction

Good morning, Chairman Coble, Congressman Scott, and Members of the Subcommittee. My name is Robert Ryan, and I am Senior Director of Government Relations for TransUnion, LLC. TransUnion is a leading global provider of consumer report information supported by more than 4,100 employees in more than 24 countries worldwide. I appreciate the opportunity to appear before you today to discuss the role of TransUnion in the credit granting process and in assisting consumers and our business customers in preventing and remediating identity theft, and additional steps that can be taken to fight identity theft.

The Role of TransUnion in the Credit Granting Process

Consumer spending makes up approximately two-thirds of the U.S. gross domestic product. A critical component of this economic driver is the availability of consumer credit. Consumers in the United States have access to a wide variety of credit from a number of sources at extremely competitive prices. Consumers rely on the availability of credit for a variety of purposes, such as the purchase of homes, cars, education, and daily needs. In fact, there is approximately $7 trillion in outstanding mortgages and other consumer loans in the United States. There is no question that our economy would suffer if consumers could not easily access credit as they do today.

It is my pleasure to explain how TransUnion plays a critical role in the economic engine of credit availability. In sum, we provide the information necessary for lenders, regardless of where they are located, to make credit available to consumers all across the United States. In order for a lender to extend a loan to a consumer, the lender must evaluate the credit risks inherent in lending to that consumer. The proper evaluation of

the consumer's credit risks allows the lender to determine whether to provide credit to the consumer and at what price. We believe that the most accurate and predictive piece of information a lender can use in evaluating a consumer's credit risk is a consumer report (also commonly called a credit report). TransUnion is in the business of providing lenders with this critical information.

The Credit Reporting Process

In order to more fully understand TransUnion's role in the credit availability process, it is important to understand the credit reporting process itself. TransUnion is a national consumer reporting agency. We are a nationwide repository of consumer report information with files on approximately 200 million individuals in the United States. The information in our files generally consists of: (i) identification information (including social security numbers); (ii) credit history; (iii) public records (*e.g.* tax liens, judgments, etc.); and (iv) a list of entities that have received the consumer's credit report from us. It is also important to clarify what is <u>not</u> in a credit report. A TransUnion credit report does not include checking or savings account information, medical histories, purchases paid in full with cash or check, business accounts (unless the consumer is personally liable for the debt), criminal histories, or race, gender, religion, or national origin.

Most of the information in our files is provided to us voluntarily by a variety of sources. Although the Fair Credit Reporting Act (FCRA) does not require anyone to furnish information to consumer reporting agencies, or have any rules on the scope or nature of such information, the law does establish certain important guidelines for those who voluntarily furnish information to consumer reporting agencies. For example, furnishers must meet certain accuracy standards when providing information to consumer reporting agencies. Furnishers must also meet requirements ensuring that the information the furnishers have reported to consumer reporting agencies remains complete and accurate. Despite these legal obligations imposed on data furnishers, lenders and others participate in the credit reporting process due to the recognized value of complete and up-to-date credit reporting. In essence, if lenders want accurate, complete, and up-to-date information on which they are to base credit decisions, they must ensure a continuing supply of such data to consumer reporting agencies.

We take great pride in our ability to collect and disseminate credit report information. In fact, TransUnion receives and processes approximately 2 billion updates to consumers' credit files each month. However, we do not distribute credit reports to just anyone. Under the FCRA, we may not provide a credit report to anyone who does not certify to us that they have a permissible purpose for such information. This protection ensures that the distribution of credit reports is made only to those with a need for such information (*e.g.* granting credit).

The Role of TransUnion in Identity Theft Prevention and Remediation

TransUnion Is Part of the Solution

Identity theft is a serious problem and TransUnion is part of the solution. Since the 1980s, when TransUnion developed the first application fraud detection suite of services for credit grantors (our HAWK® products, introduced in 1983), we have recognized that fraud through identity theft is a problem for which we can be part of the solution. We have been helping our customers detect and avoid application fraud for over 20 years, thus reducing the number of consumers affected by identity theft. In the mid-1980s we were the first consumer reporting agency to initiate the development of special procedures to assist identity theft victims, including expedited dispute verification processes and the deletion of fraudulent information. In the late 1980s we developed the innovation of a "security alert" flag on credit reports, to alert our customers to use extra caution in opening new accounts.

In 1992, we were the first national consumer reporting agency to establish a special Fraud Victim Assistance group within our organization that is solely dedicated to identity theft problems. In 1997 we began immediate suppression, at the same time the dispute investigation process was initiated, of fraud-related information on a consumer's file upon their presentation of a police report or other documentation confirming the fraud. In March 2000, this process became an industry standard.

Our identity fraud specialists work with consumers, industry, and government agencies to remediate damaged credit files as quickly as possible, to take preventive steps that reduce further victimization, and to cooperate with law enforcement authorities in their investigations and prosecutions of this crime. As we explain on our web site, www.transunion.com, our process includes posting a security alert, opting the victim out of prescreening if the victim wishes, and notifying inquirers whose inquiries were due to fraud. We are proud to have played a leadership role in the development of processes that have become national standards today and expect to continue this leadership to combat this growing crime.

In terms of preventing identity theft, our most recent business-to-business offering to combat fraud is the Fraud Management Platform. The program provides convenient access to one of the most comprehensive sets of fraud-related databases ever assembled, along with cutting edge analytics and the decisioning technology to help our clients identify fraud. Our Fraud Management Platform gives businesses and government agencies of all sizes the ability to verify and authenticate customer information, allowing businesses and agencies to detect identity thieves more easily. In other words, businesses and government agencies will be better able to determine whether the identifying information submitted by an individual is accurate, and that the individual is actually who they claim to be. We would be happy to provide the Subcommittee more detailed information about any of our fraud-prevention services upon request.

The Importance of National Standards in Combating Identity Theft: The FACT Act of 2003

The Fair and Accurate Credit Transactions Act of 2003

As you know, on December 4, 2003, President Bush signed into law the Fair and Accurate Credit Transactions Act of 2003, or the FACT Act. We applaud Congress for enacting the FACT Act, which makes permanent important national standards in the credit reporting system, and includes a comprehensive set of provisions pertaining to identity theft. I am pleased to note that many of the identity theft provisions in the FACT Act are based on innovations that TransUnion and other consumer reporting agencies have developed to help consumers in the fight against identity theft.

A significant provision in the new law is a requirement to provide free credit report annually to consumers upon request. This new obligation springs from the idea that if the credit report is free there will be increased access to credit histories by more people, and that increased access will improve accuracy and reduce identity theft by encouraging individuals to regularly review their credit reports. There remains significant debate as to the validity of this logic since credit reports were always accessible for a modest fee (currently $9) and for many years all national consumer reporting agencies have provided free credit reports, upon request, to identity theft victims and to individuals who think there may be fraudulent information on their reports.

The new law also provides for three types of security alerts in credit reports—an initial alert (upon a good faith suspicion that the individual may be subject to identity theft), a "military" alert (for our men and women serving in the military away from home), and an extended alert (in cases of actual identity theft). As a general matter, certain users of consumer reports (*e.g.* creditors) are required to take steps to confirm a consumer's identity prior to extending credit when these alerts are present on credit reports. As I mentioned above, TransUnion was a pioneer in giving consumers the opportunity to place security alerts in their credit files.

The FACT Act also codifies what has been our industry's voluntary practice concerning the immediate blocking of information related to identity theft upon the consumer's providing us with an identity theft report—usually a police report. This practice is also known as "tradeline blocking." The national consumer reporting agencies are required to share information about security alerts and blocked data among themselves, so that a consumer's actions with one consumer reporting agency will flow to the others, and be reflected on their credit reports.

The FACT Act will also benefit consumers by requiring the Federal Trade Commission to develop a summary of consumer rights under the FCRA with respect to the procedures for remedying the effects of fraud or identity theft involving credit or other financial accounts or transactions. This provision is designed to assist identity theft victims in understanding the numerous tools at their disposal, such as the use of security alerts or tradeline blocking, to mitigate the harms of identity theft. Consumer reporting

agencies will provide a summary of these rights to any consumer who contacts them and expresses a belief that he or she is a victim of fraud or identity theft involving a financial transaction.

The FACT Act also requires a consumer reporting agency to provide a "heads up" to a user of credit reports if the user submits to a consumer reporting agency an address for a consumer that does not match an address in the consumer reporting agency's files. This provision is based on existing practices used by TransUnion to notify creditors and others that the consumer's address does not match one we have on file. This serves as another protection against identity theft, where the criminal may use a victim's identification information but the criminal's address in order to obtain credit or other goods or services. Under the FACT Act, the user of a credit report that contains such a notice of discrepancy will need to take certain steps to reduce the risk that the transaction is the result of identity theft.

The issue of data furnishers providing the consumer reporting agency information that has been identified as fraudulent by the consumer reporting agency, and has been "blocked" by the consumer reporting agency, has been addressed by the FACT Act in two ways. First, in certain circumstances, the law prohibits the sale to third parties of accounts on which the creditor has received a notice of identity theft from either the consumer directly, or from the consumer reporting agency. The intent is to prevent the fraudulent information from finding its way back onto the credit report in the form of a report from a third party collection agency. Second, the FACT Act prohibits data furnishers from providing information to a consumer reporting agency if the consumer provides them an identity theft report identifying the relevant information as resulting from identity theft, or if the furnishers are notified by a consumer reporting agency that an identity theft report has been filed with respect to such information.

Furnisher Obligations

Because the FACT Act makes permanent the national standards pertaining to data furnisher obligations, it removed the danger that state laws pertaining to furnisher obligations could have reduced the number of entities willing to provide information to consumer reporting agencies. Withdrawal of data furnishers from the system would result not only in a loss of the credit information they provide but would also result in the loss of the address updates they provide. TransUnion's database relies on addresses that are in active use by creditors in mailing monthly statements to their customers. The fact that most data furnishers today also provide us with the social security number of their customers allows us to bridge address changes and name variations that commonly occur in our society. Businesses and government agencies with a permissible purpose to obtain a consumer report rely on our robust national database of names, social security numbers, and up to date addresses for a variety of fraud prevention and identity authentication services. With less current identification or address information coming into the database, the performance of these services would suffer.

Reinvestigation Timeframes

In identity theft cases, the consumer reporting agency is tasked with sorting out accurate and inaccurate information about the consumer. This is a difficult process and, if not done properly, could affect not only the consumer's ability to obtain credit but the safety and soundness of our financial institutions. We were gratified that the FACT Act preserved the national standard for reinvestigation processes and timeframes. In this regard, identity theft victims in Pennsylvania will continue to be treated no differently than victims from California to Florida. As a nation, we cannot have any other result.

What More Can Be Done?

We recognize that despite our best efforts, and the enactment of the FACT Act, that more can be done to address identity theft. This hearing is to examine more broadly any additional steps that can be taken by Congress, by law enforcement, and by holders of individuals' personal information. Allow me to respectfully offer these thoughts:

Congress

Although Congress has provided for several laws pertaining to identity theft, identity thieves can operate with the belief that, in the event that their crimes are investigated and prosecuted, the criminal penalties are not so severe as to deter their actions. We believe more can be done to find, investigate, and prosecute identity thieves and to punish them more severely. Therefore, TransUnion strongly supports H.R. 1731, the Identity Theft Penalty Enhancement Act, introduced by Congressman Carter and Congressman Schiff, and H.R. 3693, introduced by Congressman Scott and Chairman Coble. Both of these bills deserve the bi-partisan support they have received. We believe that each of these bills, by stiffening criminal penalties for identity theft crimes and increasing the resources available to investigate such crimes, would provide key tools in our fight against identity theft.

I would also like to stress the advantages of national standards regarding the protection of personal information. Most major holders of personal information are nationwide institutions. Furthermore, in our age of technology, personal information flows rapidly across state borders to serve consumers quickly and accurately. Any new federal provisions pertaining to consumer information must establish a uniform national standard to enable better consumer education and more reliable implementation by persons covered by any new law.

In considering legislation to protect personal information held in public records (or other records held by government), Congress should remember that access to this information by legitimate companies (such as consumer reporting agencies governed by the FCRA) helps to combat identity theft. The reverse is also true—to the extent consumer reporting agencies, and other legitimate businesses servicing both government and industry, are denied access to complete personal information in government records, we are hindered in our ability to combat identity theft though services such as the Fraud

Management Platform, described above. Legislation restricting access to personal information should provide appropriate exemptions for these purposes.

Law Enforcement

Many law enforcement agencies, at many levels of government, are doing excellent work in aggregating information on identity theft in order to fight the crime and to assist victims. Federally, the Secret Service, the FBI, and the FTC all have databases of identity theft information that are shared with local law enforcement. The Attorneys General of California, and other states, have their own databases of identity theft cases. The financial crimes units of many major police departments in cities like Chicago, Los Angeles and New York also have their own databases of identity fraud cases. We applaud efforts to assist all levels of law enforcement to improve communications and information sharing, in order to enhance effective prosecution of these crimes. We believe that H.R. 1731 and H.R. 3693 will improve the weapons available to law enforcement in this regard.

Second, we support efforts to improve the ease with which identity theft victims can file identity theft reports, in a way that does not promote further fraud.[1] Today at TransUnion we regularly receive fraudulent or forged police reports—it's a common tactic of credit clinics used to attempt to have accurate information removed from credit histories. We would like to see true identity theft victims have access to a more uniform means of filing genuine identity theft reports, such as through a federal law enforcement agency like the U.S. Postal Inspection Service. These standardized reports would be of use to law enforcement investigations spanning multiple jurisdictions. Such reports would also be more readily verifiable by consumer reporting agencies, and thus cut back on credit clinic abuse of the consumer reporting system.

Holders of Personal Information

We believe that legislation is needed concerning breaches of the security of personally identifiable information. In the event that personally identifiable information is compromised and obtained by unauthorized persons, we believe the holder of that information should have several responsibilities: First, if the holder of the information has reason to believe that the personal information may be used to harm the consumer to whom the information pertains, the holder should notify each person whose personal information was exposed, and the holder should coordinate with at least one of the national consumer reporting agencies (such as TransUnion) to arrange for initial alerts to be posted on those individuals' credit reports. Second, the holder of the information

[1] The FACT Act defines an identity theft report, subject to further rulemaking by the Federal Trade Commission, as a report "that alleges identity theft, that that is a copy of an official, valid report filed by a consumer with an appropriate federal, state or local law enforcement agency, including the United States Postal Inspection Service, or such other government agency deemed appropriate by the Commission; and the filing of which subjects the person filing the report to criminal penalties relating to the filing of false information if, in fact, the information in the report is false." 15 U.S.C. § 1681a(q)(4)

should have a duty to reimburse the consumer reporting agency for the costs of the postings of alerts and any subsequent file disclosures and reinvestigations.

Conclusion

At TransUnion, we are proud of our leadership in the development of processes and procedures to prevent and remediate identity theft. We applaud the 108th Congress for enacting the FACT Act, creating important new national standards that will help remediate identity theft. We are gratified that many of the provisions in that bill were based on credit reporting industry standards that TransUnion helped put in place. We also support both the intent and the substance of the two bills before this Subcommittee today, establishing stiffer penalties for aggravated identity theft, and to provide additional resources to law enforcement for combating this crime. We appreciate the opportunity to present our suggestions for additional measures which this Subcommittee may wish to consider.

Mr. Chairman, Congressman Scott, and members of the Subcommittee, I sincerely appreciate your invitation to testify today on identity theft. TransUnion looks forward to continuing to be part of the solution to this terrible crime.