TransUnion

Eric Rosenberg
Director, State Government Relations
Law Department
555 W. Adams St.
Chicago, IL 60661

Tel 312-466-6323
Email erosenb@transunion.com

April 11,2012

Statement on **Identity Theft**
Pennsylvania House of Representatives, Consumer Affairs Committee

Chairman Godshall and members of the Committee, thank you for this opportunity to appear before the Consumer Affairs Committee. For the record, I am Eric Rosenberg, Director of State Government Relations for TransUnion.

TransUnion is a nationwide consumer reporting agency, as described in Section 603(p) of the federal Fair Credit Reporting Act (FCRA), and has more than 3,100 employees with operations on five continents and in 23 countries. For more than 40 years, we have worked with businesses and consumers to gather, analyze and deliver the critical information needed to build strong economies throughout the world. TransUnion commends you for holding this hearing on identity theft and appreciates the opportunity to provide input on this subject.

Let's start by defining Identity Theft. Financial institutions like TransUnion define it as stealing someone's personal identifying information, then fraudulently using it to establish credit or take over existing accounts. It is also defined as credit cards lost, stolen or not received, or counterfeited, and fraudulent applications accounts takeovers, for example. Another type of identity theft these days is *synthetic* identity *theft,* in which identities are completely or partially fabricated. This commonly involves combining a real Social Security number with a name and birthdate other than the ones associated with the number. Synthetic identity theft is more difficult to track as it doesn't show on either person's credit report directly, but may appear as an entirely new file in the credit database or victim's credit reports.

TransUnion provides a wide array of fraud prevention, detection, and remediation products and services. For our business customers, we provide fraud and Identity management solutions to protect businesses and their customers by verify identity data and ensuring that the right customers are accessing their accounts in order to reduce risk exposure and potential losses. And, for example, in the event of a security breach, be able to react quickly and effectively to minimize the impact.

However, while the topic of identity theft is quite broad, my statement today focuses on a number of issues that have been raised in hearings and legislation over the past years that have contributed materially to the protection of consumers by establishing new duties for the consumer credit reporting industry and empowering consumers with important new rights. It bears noting that these duties and rights are all the more effective and easy for consumers to use because they are largely uniform.

It is important to keep in mind that only approximately 28% of identity theft cases involve credit or financial fraud. Phone, utility, bank and employment fraud make up another 50% of cases. To

assist victims of identity theft in a timely and effective manner and to provide a uniform experience for fraud victims, the nation's leading consumer reporting agencies long ago voluntarily initiated a comprehensive series of initiatives, which are cwered below. Many of these practices were so significant that they were codified as part of the federal Fair Credit Reporting Act - the national law regulating consumer data practices.

Background on the federal Fair Credit Reporting Act – FCRA, established in 1970, is the nation's first true federal privacy law. The touchstone of the FCRA is the accuracy obligation of consumer reporting agencies. The law requires that consumer reporting agencies maintain reasonable procedures to assure maximum possible accuracy. The FCRA also restricts access to credit reports by establishing permissible purposes for consumer reports, including for employment, credit, and insurance. It also restricts access by requiring affirmative consent of the individual and notices and opt-out for prescreened offers of credit. FCRA also provides free access upon notice of adverse action, or reasonable belief of fraud, and establishes a consumer's right to dispute inaccurate or incomplete information, while placing the burden or reverification on CRAs and data furnishers.

Consumer Rights tor Identity Theft Prevention and Remediatiop

By the end of 2004, all FACT Act amendments made to the Fair Credit Reporting Act were effective. As of this date the credit reporting industry brought online a series of nationwide practices which inure particular benefits to consumers who may have concerns about identity theft. These national standards include:

Free Annual Credit Reports - Because the information in your credit report is used to evaluate your applications for credit, insurance, employment, and renting a home, consumers may check their credit reports at each nationwide consumer reporting agency at least once per year to ensure the information is accurate and up-to-date. TransUnion has long encouraged consumers to self-monitor their credii report. Monitoring credit - by checking the credit report at least once a year to correct errors and detect unauthorized activity – is one of the best ways to spot identity theft.

Fraud Alerts – AFraud Alert is a cautionary flag, which is placed an individual's credit file to notify lenders and others that they should take special precautions to ensure the individual's identity before extending credit. When a consumer places a Fraud Alert, he or she can provide a mobile or other phone number for lenders to contact that individual to verify that the party applying for credit is actually the consumer applying, not a fraudster. These alerts were voluntarily established by TransUnion and the other nationwide CRAs in the mid-nineteen nineties. TransUnion has long believed that fraud alerts strike the right balance for consumers who wish to ensure that a lender is notified of their concerns about identity verification where they have already been or may become victims of the crime of identity theft. Consumers recognize that while these alerts can slow down credit approval processes, alerts do not stop a transaction and, thus, consumers can continue to actively seek out better financial products and services whenever they wish.

When a consumer places a Fraud Alert on the credii report with any one of the three major credit reporting companies, that company will notify the other two and fraud alerts will also be placed on those files, too. An Initial Fraud alert lasts for 90 days and may be renewed. Fraud Alerts are available at no charge to consumers who believe they may be victims of fraud.

The FACT Act created three specific types of fraud alerts.

- Initial fraud alerts stay on the consumer's report for a minimum of 90 days and will be placed on the report even when there is just a concern that a person might become a victim of identity theft. Creditors which receive this alert must take steps to form a reasonable basis that they have properly identified the consumer. Extended alerts are placed on the consumer's file when he/she presents an tdentity theft report. This alert remains on the consumer's file for a full seven years and it may include contact information for a consumer which can be used as part of the identity verification process. Most important to the codification of TransUnion's voluntary fraud-alert practice was that the FACT Act tied the presence of the alerts to specific duties for the recipients. This tying of the consumer reporting agency's duty to place such alerts with a corresponding duty for recipients to form a reasonable basis for identity verification had never previously been established and we believe that this materially improved the fraud alert systems that previously existed.
- Though similar to fraud alerts, active duty alerts may only be used by in viduals who are serving in an active duty capacity for our armed services. These alerts remain on the service member's credit report for twelve months and, like fraud alerts, are tied to duties for recipients to take steps necessary to reasonably identify the identity of the applicant before approving the application.

Address Discrepancy Indicators - The FACT Act also established additional protections for consumers in transactions even where a fraud alert might not be involved. Specifically, the FCRA require that where a nationwide consumer reporting agency receives a request from a creditor for a credit report and finds that the address submitted by the creditor diiers materially from the address on the consumer's credit report, it must indicate to the creditor that this diierence exists. Thus, lenders have an additional red flag to consider in attempting to properly validate the identity of an applicant. It is important to note that changes in addresses are not necessarily a strong indication of fraud when one considers that approximately 40 million addresses change each year in this country. Nonetheless, the FACT Act ensured an appropriate focus on address discrepancies by all financial institutions and this adds additional protection for consumers. While final regulations specifying what a recipient of an address discrepancy indicator must do with them are not completed, no doubt these indicators are being used by lenders today.

Identity Theft Reports - The FACT Act also defined the term 'identity theft report'' As a voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about id e n tii theft-related problems. This definition was a key to ensuring that victims of identity theft could avail themselves of a number of rights under the law even if they were having trouble obtaining a traditional police report. The ultimate success of this new definition is in the balance struck by the rules which ensure that such reports can be readily accessed and used by ail victims without creating a situation where the reports are hard to verify, misused or easily forged.

Identity Theft Reports and Blocking Fraudulent Data - In year 2000, TransUnion, along with our CRA counterparts, established a nationwide voluntary initiative for victims of identity theft which allowed them to submit a police report and request that fraudulent data be blocked in victims' reports. FCRA picked this concept us and codified that t a consumer, subiect to certain procedures, *can* act lo "block" specific fraud-related items (or trade lines) from appearing in his or her credit report. But trade line blocking does not prevent the issuance of a consumer credit

report; it only limits certain fraud-related information fmm being included in that report. The FACT Act codified this initiative and expanaed it by use of Me new 'identity theft report" definition. In enacting this national standard. Congress ensured that all victims received the same treatment and that fraudulent data would be removed from victims' reports.

- Red Flag Guidelines - A red flag is a pattern, practice, or specific activity that could indicate identity theft. The FCRA identifies relevant red flags and incorporates them into the requirements for financial institutions to follow. Accordingly, Financial institutions must detect red flags that are part of the Program, pespond appropriately to any red flags that are detected, and ensure the Program is updated periodically to address changing risks. Beyond the specific provisions of law discussed above, Congress recognized the need to empower regulators to develop guidance for financial institutions which is intended to encourage the use and accelerate the adoption of a robust combination of technologies and business rules to further reduce the incidence of identity theft.

  Five categorres of red flags are:
  1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers
  2. Presentation of suspicious documents
  3. Presentation of suspicious personal identifying information
  4. Unusual use of, or other suspicious activity related to, a covered account
  5. Notice from customers, victims of identity theft, or law enforcement authorities

Security Freezes – A Security Freeze is a more dramatic step to protecting information on a credit report from being released for fraudulent purposes and should not be confused with a Fraud Alert. Placing a Security Freeze will prevent lenders and others from accessing a consumer credit report entirely, which will prevent them from extending credit. A security freeze gives consumers the choice to "freeze" or lock access to their credit file against anyone trying to open up a new account or to get new credit in their name. With a Security Freeze in place, the consumer will need to take special steps when they wish to apply for any type of credit, including lifting the freeze with TransUnion, or removing the freeze altogether.

When a security freeze is in place at all three major credit bureaus, an identity thief cannot open a new account because the potential creditor or seller of services will not be able to check the credit file. When the consumer is applying for credit, he or she can lift the freeze temporarily using a PIN so legitimate applications for credit or services can be processed.

Because of more stringent security features, a Security Freeze is placed and maintained separately with each of the three major credit reporting companies. A Security Freeze remains on the consumer's credit file until you remove it or choose to lift it temporarily when applying for credit or credit-dependent services.

In Pennsylvania, consumers who are victims of identity theft, or believe they may have been a victim of identity theft, are able to freeze their credit file for no charge. In addition, consumers 65 years of age and older are able to freeze their credit file for no charge. Otherwise consumers in Pennsylvania are charged $10 to place and lift the freeze.

The fact that the provisions just discussed all operate as national standards bears repeating. The Congress was prescient in recognizing that fraud prevention and, in fact, regulation of a nationwide system of credit reporting and credit markets is best handled through uniform

national standards. A series of state laws which impede the free flow of information across this country cannot possibly achieve the same benefit for all cit'iens wherever they may live. We applaud the Committee for the necessary focus on the needs of consumers and identity theft victims through the establishment of national standards of practice.

In closing our discussion of national standards under FCRA, I am reminded of the fact that the FCRA itself remains the only law which directly regulates consumer reporting aencies. The national standards reauthorized and established by the FACT Act were critical to our nationwide companies and it remains vitally important that those operating as consumer reporting agencies are regulated under this single set of national standards, law and regulation

Recommendation

Partner with private industry to prevent and remediate child ID Theft – Unfortunately, children's personally identifying information makes a tempting target for identity thieves – theft of a child's identity may go undetected for years. Most parents apply for a Social Security Number after a new baby is born, which is all that's required to open most credit accounts. It could be years until a child applies for credit in his/her own name – that allows years for an identity theft to go undetected. And that could create serious consequences. Identity theft will affect the child's credit and employment history if the thieves (who sometimes turn out to be family members), obtain credit accounts or even get jobs. If the thieves are arrested for other crimes, those crimes could become associated with the child's record.

We recommend that, at a minimum, the Pennsylvania Attorney General's office replicate what the AGs office in Utah announced in February. Together with TransUnion, the Utah AGs office announced an unprecedented new program to help protect children from identity theft. The Child Identity Protection Program (CIP), features a secure online site through which Utah parents and guardians can register their minor children for the protection at no cost. This is a groundbreaking public/private partnership dedicated to specifically protecting children from having their good names and future credit ruined by identity thieves. TransUnion has worked closely with Utah to pioneer this program and our hope is that other states across the country are motivated to engage in similar efforts.

Designed to help prevent identity thieves from using the personal identifying information of children in the issuance of credit, the CIP program enables Utah parents or guardians to enroll their children by providing name, address, date of birth and Social Security number information securely online. Once enrolled, TransUnion adds each minor's SSN to a database it uses to alert creditors about potential fraud risk when requests for credit reports are received. This protection remains in place until the minor reaches 17 years-of-age. Additionally, if TransUnion determines that a credit file containing both the minor's SSN and name has, in fact, been created, steps are also taken to ensure that the TransUnion file is purged of any fraudulent information and cannot be accessed until the minor's 17th birthday. Our hope is that our efforts here will help to build momentum for involvement from the Federal Government and in particular the Social Security Administration, whose participation could significantly speed the process of stamping out child ID theft in this country once and for all.

In sum, there are a number of existing avenues available for consumers to detect, prevent, and rernediate fraud, including security freezes, fraud alerts and blocking tradelines. But we still have a long ways to go to help fight child ID theft. With these in procedures in mind, we look forward to working with the Commonwealth of Pennsylvania on more creative identity theft solutions. Thank you again for inviting me to speak today, and I am available for any questions.