OPENING REMARKS OF THE HONORABLE RUBEN HINOJOSA
HOUSE COMMITTEE ON FINANCIAL SERVICES
"ASSESSING DATA SECURITY: PREVENTING BREACHES AND PROTECTING SENSITIVE INFORMATION"
MAY 4, 2005

Chairman Oxley and Ranking Member Frank,

I want to express my sincere appreciation for you holding this very important and timely hearing today. Having served as one of the Members of the Task Force on Identity Theft that contributed substantially to the language ultimately included in the FACT Act of 2003, I am very disturbed by the recent events that have endangered the personal privacy of many of our constituents, including over 300,000 in the Lexis-Nexis case alone.

For weeks, the media has reported on the rampant loss of financial information of Americans from coast to coast. What at first seemed to be isolated incidents of theft now seems much larger and has impacted customers of well-known companies like Ralph Lauren, DSW Shoes, Lexis-Nexis, and others. The frightening part of this lapse in security is that millions upon millions of people are now exposed to possible identity theft.

Identity theft can be devastating for consumers and can destroy their credit, their financial security and their sense of protection and well-being. Similar to a home invasion or robbery, victims of identity theft are exposed to the whims of those who stole their personal financial information. Identity theft tends to occur when an imposter steals a victim's personal information to gain credit, merchandise and/or services in the victim's name. It is the most common complaint received from consumers in all 50 states; and, my home state of Texas ranks third in the number of identity theft victims.

According to the Federal Trade Commission, identity theft occurs when an individual's Social Security number, credit card number(s), or name is used without permission or knowledge. Perpetrators of identity theft often use this information to open credit card accounts, utility services, or to use already existing accounts.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years – and their hard-earned money – cleaning up the mess thieves have made to their good name. Victims of identity theft may incur unauthorized charges to their credit cards and unauthorized withdrawals from bank accounts. Victims may lose job opportunities, be unable to secure a loan, obtain a mortgage, or get arrested for crimes they didn't commit.

What's more frightening, is this crime often goes undetected. Most people aren't aware that they may have been victimized and that their accounts have been compromised until it's too late.

While it could be quite difficult to determine if you have been a victim of identity theft, there are a few warning signs. You may fail to receive bills or other mail, receive credit cards you didn't apply for, or receive calls from creditors or businesses about merchandise you didn't order or request. You can request, once annually, a free copy of your credit report, which contains vital information about your credit history. This new benefit is being implemented on a rolling basis.

As a member of the House Task Force on Identity Theft and co-founder and co-chair of the Financial and Economic Literacy Caucus, it is a priority for me to educate consumers about this very important issue – especially in light of these recent news reports. Many Americans are not aware of their rights and do not have a grasp of their own personal finances; thus, making them vulnerable to identity theft. I have been encouraging my constituents to begin taking the necessary steps to educate themselves about everything from how to fill out a loan application to understanding their own credit report.

However, I keep stressing that they do not have to sit idly by – they can prevent identity theft. They can tear or shred their receipts, copies of credit applications or offers, insurance forms, check and bank statements, and expired credit cards; keep their Social Security card in a safe place, and give their number only when necessary; pay attention to their billing cycles; do not write their PIN numbers on their credit or debit card; and, ensure that information they share on the Internet is with a legitimate institution or vendor.

And if they happen to find themselves a victim of identity theft, there are steps they can take immediately. Contact the fraud department of one of the three major credit bureaus – Experian, TRW, and TransUnion. As soon as the credit bureau they contact confirms the fraud alert, the other two credit bureaus will be automatically notified, and all three credit reports will be sent to the victim immediately. In addition, they should also close all tampered accounts, file a police report and file a complaint with the Federal Trade Commission.

I have informed my constituents that, for more information on what they can do if they believe their identity has been compromised, contact their local authorities or the Federal Trade Commission at (877) 438-4338 or www.consumer.gov/idtheft.

The Department of Justice www.usdoj.gov/criminal/fraud/idtheft/html and/or

BITS Financial Services Roundtable www.bitsinfo.org/ci_identity_theft.html

The purpose of today's hearing is to examine a number of recent data security breaches to determine how consumers' personal and financial information was stolen and what actions have been taken to minimize unauthorized use of the stolen information. The first thing we need to know are the facts surrounding the breaches.

According to Committee staff and to various press reports and press releases from the underlying entities, data thieves employed a variety of means to gain unauthorized access

to consumers' private information. These include both high-tech means for stealing computer access codes and passwords, as illustrated in the various university and retail store security breaches, as well as such low-tech methods as impersonating legitimate business clients, as in the ChoicePoint and Lexis-Nexis examples. Other security breaches involved more traditional forms of theft, such as the theft of computers and computer backup tapes in the Wells Fargo Mortgage and Bank of America examples.

The largest known security breach of financial data became public in February 2003 when the FBI announced a nationwide investigation of a breach of a computer database containing roughly 8 million Visa, MasterCard and American Express credit card numbers.

Officials of British-based HSBC PLC notified at least 180,000 credit card customers in mid-April 2005 that their account information may have been obtained in a security breach of the computer database of a national retailer.

DSW announced in April, 2005, that computer hackers had obtained account data from 1.4 million credit cards used by customers at 108 retail stores between November 2004 and February 2005. Checking account numbers and driver's license numbers where also stolen from nearly 95,000 customer checks.

Lexis-Nexis Group announced in mid-April 2005 that files containing social security numbers, driver's license numbers and other detailed personal information on 310,000 consumers had been illegally obtained by persons posing as legitimate business customers.

Officials of the University of California-Berkeley announced in April 2005 that a laptop computer containing information on 98,000 students and alumni had been stolen a month earlier. The computer contained unencrypted personal information including social security account numbers, birth dates and home addresses.

In March 2005, Boston College notified 106,000 alumni that a hacker had gained access to a computer database containing their personal information.

In February 2005 Bank of America announced that it lost computer backup tapes containing personal information, including social security account numbers and credit card accounts data, relating to 1.2 million federal workers, including many Senate office accounts.

The Chief Executive of Georgia-based ChoicePoint Inc. announced in mid-February 2005 that criminals posing as legitimate small businesses had obtained sensitive personal information on 145,000 American consumers during the summer and fall of 2004 and that at least 750 of them had been defrauded.

As a result of these thefts, several bills related to identity theft have been introduced during the 109th Congress.

H.R. 1099, the "Anti-Phising Act of 2005", would make it a federal crime to knowingly create or procure the creation of a website or domain name that represents itself as a legitimate online business, without the authority or approval of the registered owner of the actual website or domain name of the legitimate online business; and use that website or domain name to induce, request, ask, or solicit any person to transmit, submit, or provide any means of identification to another. It would also be a crime to send a message that falsely represents itself as being sent by a legitimate online business for the purposes listed above. The penalty for each could be a fine, imprisonment for five years, or both.

H.R. 1078, the "Social Security Number Protection Act of 2005", would direct the Federal Trade Commission to promulgate regulations to impose restrictions and conditions on the sale and purchase of social security numbers.

H.R. 220, the "Identity Theft Prevention Act of 2005", would repeal provisions of the Social Security Act authorizing various uses of the social security number. The bill would also require all social security numbers to be randomly generated, make the social security number the property of the individual to whom it is issued, and prohibit the Social Security Administration from disclosing the number to any agency or instrumentality of the federal or state government. The federal government would also be prohibited from issuing government-wide identifying numbers or establishing a uniform standard for identification of an individual that is required to be used by any other federal agency, state agency, or private person.

Although the federal financial regulatory agencies and credit-card industry have been attempting to find ways to address the security breaches, I believe that additional hearings are needed to review the effectiveness of the identity theft provisions set forth in the FACT Act and to oversee the regulatory agencies' implementation of those provisions. I am not certain that legislation, such as that cited above, is needed at this time to address the current security breaches. However, I think that this Committee needs to continue its oversight role and to remain vigilant to ensure that we do all in our power to ensure that consumers' identities are not stolen, and, if they are, to provide the fastest remedy possible.

I look forward to the testimony of today's witnesses, and I yield back the remainder of my time.