

**OPENING REMARKS OF THE HONORABLE RUBEN HINOJOSA
HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
“ENHANCING DATA SECURITY: THE REGULATORS’ PERSPECTIVE”
MAY 18, 2005**

Chairman Bachus and Ranking Member Sanders,

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.

As I noted during last week’s hearing, 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.

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 were also stolen from nearly 95,000 customer checks.

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 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.

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 be arrested for crimes they did not commit. According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions \$48 billion and consumers \$5 billion. Victims pay an average of about \$1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports.

Victims do not have to sit idly by – they can defend themselves against 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.

Furthermore, our constituents can access websites such as the BITS website created by the Financial Services Roundtable. The website helps consumers become aware of the many steps they can take to safeguard their personal information. The tips on the BITS website were adapted from the BITS white paper “Financial Identity Theft: Prevention and Consumer Assistance.” The website provides guidance on how to protect your Social Security numbers and cards; your credit cards; your identity from predators on the Internet; your mail; and other topics. All of these documents are printed on the BITS website and available for download. You may access the website at www.bitsinfo.org/ci_identity_theft.html.

Having noted all of the aforementioned, the question becomes one of what, if anything, can or should Congress do to address the increasing numbers of identity theft and protect our constituents.

Yesterday, I received a letter from Consumers Union highlighting its “Have You Heard?” Column from the June 2005 *Consumer Reports*, which addresses the critical issue of identity theft. There are several recommendations in that column that I found very compelling. One of them focuses on preventing breaches from happening in the first place. It stresses how critical it is to impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available, and require creditors to take additional steps to verify the identity of an applicant when there is a sign of possible ID theft. Moreover, it recommends that Congress act to restrict the sale, sharing, posting, display, and secondary use of Social Security numbers. I ask that a copy of this letter and the column,

attached at the end of my opening remarks, be included in the official Subcommittee record.

Several bills have been introduced this Congress to address identity theft. H.R. 1078, the “Social Security Number Protection Act of 2005”, introduced by Congressman Markey, caught my attention. It would direct the Federal Trade Commission to promulgate regulations to impose restrictions and conditions on the sale and purchase of social security numbers. I hope that today’s witnesses will comment on this legislation, and I encourage my colleagues in the Committees on Energy and Commerce and Ways and Means, to which the legislation was referred, to hold hearings on it.

Finally, I look forward to the testimony of today’s witnesses in the hope that they can provide further insight into the “Bank Data Breach Guidance” the Federal bank regulators published in the *Federal Register* on March 29, 2005; a similar guidance issued by the National Credit Union Administration; and an explanation as to why the FTC has yet to issue a similar guidance.

Having said that, Mr. Chairman, I yield back the remainder of my time.



Nonprofit Publisher
of Consumer Reports

Re: Need for strong identity theft legislation

May 17, 2005

Members, Subcommittee on Financial Institutions and Consumer Credit
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

Dear Representative:

In anticipation of tomorrow's subcommittee hearing on the security of our personal information, Consumers Union, the non-profit, independent publisher of *Consumer Reports*, would like to highlight to you the attached "Have You Heard?" Column from the June 2005 *Consumer Reports*, which addresses the critical issue of identity theft.

Identity theft is a serious crime that has become more common in recent years as we have delved further into the "information age." According to the Federal Trade Commission, 27.3 million Americans have been victims of identity theft in the past five years, costing businesses and financial institutions \$48 billion and consumers \$5 billion. Victims pay an average of about \$1,400 (not including attorney fees) and spend an average of 600 hours to clear their credit reports. The personal costs can also be devastating; identity theft can create unimaginable family stress when victims are turned down for mortgages, student loans, and even jobs.

As recent scandals involving ChoicePoint, Lexis-Nexis, and others have illustrated, American consumers cannot fully protect themselves against identity theft on their own. Congress must act to protect our personal information from identity thieves. Specifically, Congress should:

Prevent breaches from happening in the first place.

It is critical to impose strong requirements on information brokers to protect the information they hold and to screen and monitor the persons to whom they make that information available, and require creditors to take additional steps to verify the identity of an applicant when there is a sign of possible ID theft. In addition, Congress should act to restrict the sale, sharing, posting, display, and secondary use of Social Security numbers.

- **Require notice of breaches of sensitive information.**

Congress must impose requirements on businesses, nonprofits, and government entities to notify consumers when an unauthorized person has gained access to sensitive information pertaining to them. Consumers need prompt and proper notice, including information on what kind of data has been stolen.

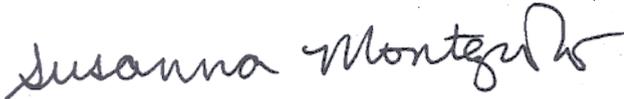
- **Ensure that victims have rights, too.**

Currently, when a company improperly breaches a consumer's sensitive information, the onus is on that consumer – the victim – to fix the problem. Congress can do much to change this and to empower consumers who are at risk for or who already are victims of identity theft, such as by strengthening the protections of the Fair and Accurate Credit Transactions Act (FACTA). FACTA can be made more effective by extending the initial fraud alert period from 90 days to one year, automatically sending consumers with a fraud alert a free credit report, and giving consumers who receive a notice of a security breach the right to an extended fraud alert.

Congress should also authorize federal, state, and private enforcement and provide funding for law enforcement to pursue multi-jurisdictional crimes promptly and effectively. Victims also need tools to fix the problem once the breach occurs – such as making sure there is a clear process for preventing identity theft and repairing credit once a breach occurs, providing for free credit monitoring, and covering the costs of fixing the problem.

Thank you for your time and consideration. If you would like more information, please do not hesitate to contact us at (202) 462-6262.

Sincerely,



Susanna Montezemolo
Policy Analyst



Chanelle Hardy
Esther Peterson Fellow

Consumer Reports

JUNE 2005

EXPERT • INDEPENDENT • NONPROFIT

Have You Heard?

THE FIGHT AGAINST IDENTITY THEFT

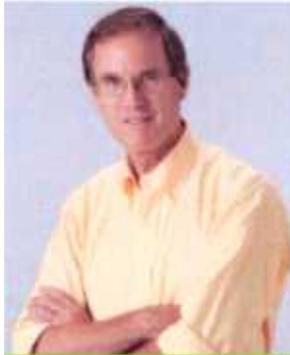
"I was mugged once, years ago," one of our editorial researchers told me. "It was bad, but at least that guy had the guts to look me in the eye." This time, she'd gotten a call from her bank alerting her that someone in Oregon had just withdrawn \$2,000 from her account. Since she and her husband were both at home in New York, that was very bad news.

Like many of the estimated 10 million people a year whose lives and accounts are invaded by identity thieves, our staffer had been as cautious as she could be and still be part of today's marketplace. But either her financial records were leaked or a hacker typed his or her way through the barriers protecting her account.

In either case, companies who hold sensitive personal and financial information about us, and the lawmakers who should be overseeing them, are failing to build stronger protections against the increasingly prevalent crime of ID theft. Lawmakers and regulators must work fast. Here are three things that Consumers Union, the publisher of *CONSUMER REPORTS*, is pushing them to do:

- Oversee information brokers, companies that collect and sell people's personal and financial data. Federal law should require them to safeguard those data, sell data only to carefully screened clients, tell consumers what's in their files, and correct mistakes promptly, since mistakes can lose you a job, a mortgage, or an insurance policy.
- Pass strong federal and state laws that require companies to notify the consumers whose personal and financial information they hold when their privacy is compromised. Now, only California residents have that protection.
- Pass laws in every state allowing consumers to "freeze" their credit-bureau files. With a security freeze in place, your credit report and score can't be given to potential new creditors unless you choose to "unlock" the file when you apply for, say, a car loan. Most businesses won't issue new credit or loans without first checking credit records. This way, thieves will hit a brick wall trying to open an account in your name.

There's no single solution to shielding consumers from the fast-changing schemes of ID thieves, so Congress should preserve the right of states to continue developing ever more sophisticated guards. For more about what CU is doing, and for what you can do to protect yourself, go to our Web sites www.consumersunion.org/privacy and www.consumersunion.org/money.



FREEZE THIEVES The right to "freeze" your credit files would stop others from opening accounts in your name.

Jim Guest

Jim Guest
President