Opening Statement

Chairman Michael G. Oxley

House Committee on Financial Services

Assessing Data Security:
Preventing Breaches and Protecting Sensitive Information

May 4, 2005

This morning, the Committee meets to consider a topic we've been hearing about on an almost daily basis during the past few months: data security and its connection to the crime of identity theft. Several recent high-profile security breaches have focused public attention as never before on the vulnerabilities of companies' data security systems. Congress now has to ask, "Are we doing enough to protect against the theft and misuse of sensitive commercial information on consumers?"

Protecting sensitive information is an issue of great importance for all Americans. In recent years, criminals in the United States and abroad have become increasingly inventive in finding ways to access and exploit information systems in order to commit identity theft.

According to a Federal Trade Commission estimate, over ten million Americans are victimized by identity thieves each year, costing consumers and businesses over $55 billion per year, not counting the estimated 300 million hours spent by victims trying to repair damaged credit records. The financial costs are staggering, with over $10,000 stolen in the average fraud.

The Financial Services Committee has worked tirelessly over the past several Congresses to identify and enact solutions to this destructive crime. During the 108th Congress, over 100 witnesses came before this Committee to testify on the reauthorization of the Fair Credit Reporting Act. Through that process, under the leadership of the gentleman from Alabama, Mr. Bachus, the Committee developed an exhaustive record on the need to increase safeguards designed to protect consumers and businesses alike from identity theft.

Through bipartisan cooperation in this Committee, we ultimately produced strong consumer protection and anti-identity theft legislation known as the Fair and Accurate Credit Transactions Act, or FACT Act.

The FACT Act places new obligations on financial institutions to prevent identity theft, entitles consumers to a free annual credit report from each of the three major credit bureaus, and creates a national fraud alert system to simplify a consumer's ability to detect and report fraudulent activity. The FACT Act was signed into law on December 4, 2003, and is currently in the process of being fully implemented by Federal regulators and the financial services industry.

The Federal banking regulators have also been hard at work on other initiatives to protect sensitive information. On March 29, 2005, the Federal Reserve, FDIC, OCC and OTS issued final data security standards for depository institutions, as required in Title V of Gramm-Leach-Bliley. The standards call for every financial institution to implement a response program to address incidents of unauthorized access to customer information maintained by the institution, and to notify the affected customer as soon as possible.

In light of continuing guidance from the regulators, it is my hope that we can focus today on the broader issue of data security, and how best to protect sensitive information from being improperly accessed, and ensure that consumers receive prompt and effective notice when sensitive information **has** been compromised and is likely to be misused. One of my concerns in this regard is that, given the dramatic rise in recent reports on data breaches, there will be a head-long rush toward notification in **every** instance.

When no evidence surfaces to indicate that their information has been misused, consumers may begin to ignore these notices as just that many more pieces of unsolicited junk mail.

California recently enacted legislation requiring disclosure of any data security breach to any state resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Only a small percentage of these cases, however, have actually resulted in any fraudulent activity. Other States are considering legislation similar to California's. It is important that this Committee take a look at what is being contemplated in the States and consider whether a national breach notification standard would work best for American consumers.

I would like to welcome our witnesses to today's hearing. I look forward to hearing your testimony and working with you to find ways to prevent future data security breaches and continue our efforts to combat identity theft.