

**OPENING STATEMENT OF REP. SUE KELLY**

**CHAIRWOMAN**

**SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS**

**"Fighting Fraud: Improving Information Security"**

**April 3, 2003**

Personal information must be safeguarded throughout our national credit system. Just as consumers shred their unwanted mail and take care with their receipts, financial institutions must develop and upgrade their information security procedures to protect consumers.

Financial records such as credit card numbers, combined with other pieces of personal information, are the first targets of identity thieves. Years of work are often necessary from both consumer and business victims to correct damaged credit histories and restore access to credit.

Today two Subcommittees will hear from witnesses on three specific case studies to review current industry practices and to ensure that proper security procedures and protocols are in place or are being implemented:

Teledata Communications is a company in my home state of New York that enables businesses to access credit bureau information so they can grant credit to consumers. An employee inside the company allegedly stole and sold passwords and codes for accessing credit reports for thousands of people. According to law enforcement, his actions resulted in millions of dollars of financial theft.

TriWest Healthcare, an important healthcare provider for our active duty military personnel, honored veterans, and their dependents, suffered the physical theft of its computer hardware. The equipment stored personal information about many heroes now involved in the war to liberate Iraq, including the Chairman of the Joint Chiefs of Staff, General Richard Myers. Fortunately, quick action by the company and the credit bureaus appears, thus far, to have prevented misuse of the information.

Another company, Data Processing International in Nebraska, saw its database of millions of credit card numbers hacked from the outside. It again appears that rapid action, this time by the company and the credit card companies, has prevented improper use of the numbers to date.

Through the examination of these cases, the Subcommittee will review how credit issuers, third-party vendors that process transactions, credit bureaus, and law enforcement agencies coordinate efforts to limit harm to consumers when data security is breached. Among our witnesses are officials of the law enforcement and regulatory agencies involved with these and other such cases; representatives of the companies involved; one of the most famous computer hackers in the world, now a consultant; and an expert in privacy.

I want to thank my distinguished colleague, Representative Spencer Bachus, the Chairman of the Subcommittee on Financial Institutions and Consumer Credit, for joining with me to hold this important joint hearing of our subcommittees. I also want to congratulate him for his leadership in the bipartisan passage of H.R. 522, the “Federal Deposit Insurance Reform Act of 2003,” by the full House yesterday.