OPENING STATEMENT OF CHAIRMAN SPENCER BACHUS
"FIGHTING FRAUD: IMPROVING INFORMATION SECURITY"
APRIL 3, 2003

Thank you, Chairwoman Kelly, for convening this joint hearing of our two subcommittees to review issues related to the security of personal information. This is an issue of critical importance to the financial services industry, and I believe this hearing is a timely one. This hearing, which is titled "Fighting Fraud: Improving Information Security" is one of many hearings that will be held by the Subcommittee on Financial Institutions and Consumer Credit regarding the security of personal information. I expect that at some point our efforts will culminate in comprehensive legislation addressing the broad issue of how secure consumers feel with respect to their personal information.

Today's hearing will focus on three cases where sensitive personal information was compromised through hacking or physical theft of computer databases. Each case that we will hear about today is illustrative of a different type of security breach – an outside computer hacker, employee misconduct and a garden variety burglary. Using these cases, we will review how credit issuers, third-party vendors that process transactions, credit bureaus, and law enforcement coordinate efforts to limit harm to consumers when data security is breached.

Fighting fraud and protecting the security of personal information is a topic that unites financial institutions and consumers: each group is harmed by the fraudulent use of personal information. Financial institutions are the victims of fraud because the financial institution is usually liable for any losses suffered as a result of the fraud. Consumers obviously suffer unnecessary inconvenience and insecurity as a result of fraud, and they can be exposed to additional crimes such as identity theft. Furthermore, at least a portion of financial institutions' fraud losses can be expected to be passed on to consumers in the form of higher prices. There can be no doubt that when fraud is committed, everyone loses.

For obvious reasons, financial institutions take precautions to prevent fraud, including precautions to protect the security of personal information. In addition to the self interest financial institutions have in minimizing their fraud losses, Congress has required financial institutions to maintain appropriate standards relating to information security, including standards to protect against unauthorized access to a financial institution's customer records, as part of the Gramm-Leach-Bliley Act. The requirements, as adopted by the federal banking agencies, also require financial institutions to oversee their relationships with third party service providers, including having the service providers agree by contract to implement a comparable information security program. It is my understanding that the federal banking agencies have been examining financial institutions with respect to their compliance with these requirements. However, I remain interested in learning more about the role service providers play with respect to information practices, and their ability to maintain appropriate information security programs. It is my understanding that the Bank Service Company Act gives the banking regulators broad authority to examine third-party providers. Two of the cases today illustrate that greater oversight of these entities may be necessary.

As part of the Gramm-Leach-Bliley Act, Congress also enacted stiff prohibitions against a practice known as "pretext calling," which is a fraudulent means of obtaining an individual's personal information. Pretext callers contact a financial institution's

employees and attempt to obtain customer information, usually while posing as the customer whose information they are trying to collect. This is a serious issue, and one which this committee has held several hearings previously. I am interested in learning more about efforts to enforce this prohibition and the Federal Trade Commission's views on the amount of resources devoted to fighting this fraudulent practice.

[Congress has not been the only interested governmental party with respect to information security and fraud prevention. The banking agencies have also taken proactive steps to ensure that consumers and financial institutions are protected against fraudulent and criminal activity. For example, in order to assist financial institutions in adopting the appropriate security measures, the banking agencies have jointly issued exam guidance with respect to their information security guidelines. The banking agencies have also jointly issued guidance with respect to customer authentication in an electronic banking environment. The Comptroller of the Currency has also issued bulletins or advisory letters on managing risks that may arise from business relationships with third parties, on identity theft and pretext calling, and on network security issues.]

We will also hear this morning from federal law enforcement agencies about their approach to countering those who would compromise the security of personal information. It has always been my experience that law enforcement and the financial services industry work well together with respect to pursuing those who attempt to commit crimes against consumers and financial institutions. I look forward to hearing about law enforcement's perspective on this important topic, especially with respect to whether the representatives from the FBI, Secret Service, and FTC believe they have been given the proper resources to investigate financial crimes.

In short, financial institutions, Congress, the federal banking agencies, and law enforcement have been working to address information security and fraud prevention issues. Regardless of the great pains taken by all of these parties to protect the security of personal information, the chance remains that a breach may occur. Therefore, Congress must remain vigilant to ensure that existing requirements are implemented appropriately and examine whether new safeguards are necessary. Furthermore, it is just as important for financial institutions to have mitigation plans in place in the event that their information security program is hacked or otherwise compromised. I am pleased that we will hear from several witnesses today who will describe how various parties took action to address recent data security breaches and prevent subsequent fraud.

Before we proceed, I believe that it is important to mention that although this hearing is a public forum, we should avoid discussing specific details which may give criminals ideas, or even a roadmap, for doing further harm.

Let me close by thanking Chairman Oxley for recognizing the importance of improving the security of personal information and scheduling this hearing. We must continue to work to improve security and protect sensitive data to ensure that consumers continue to have confidence in our nationwide credit system as well as our financial services system in general. I look forward to working with the Chairman, Mrs. Kelly, and my other colleagues as we continue to examine this complicated issue.

I yield back the balance of my time.