Barbara Desoer
Global Technology, Service & Fulfillment Executive
Bank of America

Written Testimony to the Financial Services Committee of the United States House of Representatives Public Hearing to Assess Data Security
Washington, D.C.
May 4, 2005

Chairman Oxley, Congressman Frank, Committee Members, good morning.

I am Barbara Desoer, Global Technology, Service & Fulfillment executive for Bank of America. I am a member of Chairman and CEO Ken Lewis' executive leadership team.

On behalf of the leadership of our company and all Bank of America associates, thank you for the opportunity to appear before this committee to provide our perspective on the loss of computer backup data storage tapes reported by Bank of America earlier this year.

I would like to express how deeply all of us at Bank of America regret this incident. We collectively make our living and pursue our professional mission by helping people at home, in business and in government manage their financial lives. This work rests on a strong foundation of trust, more so in today's incredibly complex and fast-moving world of electronic commerce than ever before. One of our highest priorities, therefore, is building and maintaining a track record of responsible stewardship of customer information that inspires our customers' confidence and provides them peace of mind.

In my remarks today, I will provide an overview of:

1. What we know regarding the loss of our computer data backup tapes;
2. The steps we have taken to alert and protect our government charge cardholders;
3. Our information security practices; and,
4. Our thoughts regarding new legislation or regulations to improve the security of personal information in our country.

On February 25, 2005, Bank of America began proactively communicating to U.S. General Services Administration (GSA) SmartPay® charge cardholders that computer data backup tapes were lost during transport to a backup data center. The missing tapes contained customer and account information for approximately 1.2 million government charge cardholders. The actual data on the tapes varied by cardholder, and may have included name, address, account number and social security number.

The shipment took place on December 22, 2004. A total of 15 tapes were shipped. Five were lost in transit. Two of the lost tapes included customer information; the remaining three contained non-sensitive, back-up software.

Backup tapes such as these are created and stored at remote locations as a routine industry contingency practice in the case of any event that might interrupt our ability to serve our customers. This is standard industry practice, and is designed to protect businesses, their customers, and the U.S. economy at large, in the event of disruptions in the economic environment that arise from either natural or man-made causes. Such contingency planning is a fundamental part of our enterprise risk management program.

As is our standard practice, none of the tapes or their containers bore any markings or information identifying our company, the nature of their contents or their destination. Nor were any of the personnel involved in the shipping process aware of the nature of the materials being shipped. As to the tapes themselves, sophisticated equipment, software and operator expertise are all required to access the information. In addition, specific knowledge of the manner in which the data is stored – that is, the "fragmented" nature of the data and the steps required to reassemble it – would be required.

After the tapes were reported missing, Bank of America officials notified appropriate officials at the GSA. Bank of America officials also engaged federal law enforcement officials at the Secret Service, who began a thorough investigation into the matter, working closely with Bank of America.

Federal law enforcement initially directed that to preserve the integrity of the investigation, no communication could take place to the public or the cardholders. Doing so would have drawn enormous public attention to the tapes at a time when their whereabouts were still a matter of intense investigation and the specific content was still being analyzed. While the investigation was moving ahead, we put in place a system to monitor the affected accounts and, in fact, researched account activity retroactively to the date of the data shipment to identify any unusual or potentially fraudulent activity in the accounts.

The investigation, which continues today, included a detailed review of the entire transit process for the shipment, including the archive vendor, truck drivers, airline personnel and Bank of America employees. The Secret Service has advised GSA management and us that their investigation has revealed no evidence to indicate that the tapes were wrongfully accessed or their content compromised. The Secret Service findings are complemented by the Bank of America fraud monitoring process, which continues to indicate there has been no unusual activity, or attempted unauthorized use of the monitored accounts to date.

In mid-February, law enforcement authorities advised us that communication to our customers would no longer adversely impact the investigation. Following our initial cardholder notifications mentioned earlier, we continued to communicate with our customers to ensure they understood the additional steps we continue to take today to help protect their personal information and to assist them with any questions they have. With multiple mailings to cardholders with information on the tapes, this amounted to several million pieces of mail.

As part of our initial communications to cardholders, Bank of America also quickly established a toll-free number government charge cardholders could use to call with questions or request additional assistance. We offered credit reports and enhanced fraud-monitoring services to cardholders at our expense. In an effort to be extra cautious and open with our customers, we also communicated to government cardholders whose account information was not included in the lost tapes.

Government cardholder accounts included on the data tapes have been and will continue to be monitored by Bank of America, and government cardholders will be contacted should any unusual activity be detected. No unusual activity has been observed to date. Per standard Bank of America policy, government cardholders will not be held liable for any unauthorized use of their cards.

In 2002, the Treasury Department chose our company to establish and chair the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. We also are a member of the President's National Security Telecommunications Advisory Committee, which provides subject matter expertise to study issues vital to advancement of national security and emergency preparedness.

I mention this evidence of our leadership not simply to highlight our accomplishments. We all agree this is a time for humility, and we've come here in that spirit. Rather, I wish only to demonstrate to the committee the seriousness with which we regard these issues and the gravity with which we regard our responsibility for leadership.

Without a strong foundation of trust and confidence, our industry cannot function and cannot serve our customers. We understand all too well this fact and its implications for our business, our economy and our country.

Our information security standards are based on regulatory guidance from the federal government (such as the OCC, the FRB and others) and international banking regulatory bodies (such as the BASEL II accord and international standards for information security controls). In addition, the bank's strategy includes a continuous review of information security assessment criteria used by industry information security professionals. It is the bank's goal to meet or exceed information security standards and regulations dictated by our regulators or used by our industry peers in our day-to-day operations.

In that spirit, I'd like to provide a brief overview of our Corporate Information Security Program. The Bank of America Corporate Information Security Program is designed to:

- Develop and implement safeguards for the security, confidentiality, integrity and availability of customer information;
- Achieve protection of information against threats to security based on the value of the information or the harm that could result to a customer from unauthorized access;
- Monitor and respond to attempts to threaten the security of customer information;
- Develop and implement plans to provide backup systems to prevent information damage or destruction caused by environmental hazards or malicious actions; and,

- Adjust the Bank of America Corporate Information Security Program in response to changes in technology, information sensitivity, threats, or the business environment.

As a national financial institution, we are highly regulated and regularly examined on our practices regarding security of customer information. We are required to follow specific regulatory guidance from the Office of the Comptroller of the Currency on how to handle such information. And we are constantly working to enhance the systems we use to monitor customer data to ensure that we know where that data is and how it is being used.

The incident we're discussing was unfortunate and regrettable. That said, we feel that it has shed helpful light on a critical element of the industry's practices for data transport. We view this as an opportunity to learn and to lead the industry to better answers that will give our customers the confidence and security they deserve. Within Bank of America, we have taken recent steps to further safeguard the secure transport of customer data, including the launch of corporate-wide package delivery carrier services for backup data tape transport.

We also acknowledge that in today's environment, in which information security issues or concerns are highly visible, there is a general belief that something must be done. I would like to assure the committee that things are indeed being done, and speaking for Bank of America, that we consider information protection among the highest priorities at our company and we take our responsibility for safeguarding it very seriously. Our annual investment in information security technology, personnel and assessment requires significant financial resources, however, it is an investment we make without hesitation and as tangible proof of the seriousness with which we treat our responsibilities.

With respect to legislative solutions currently under discussion, our recent actions demonstrate our belief that customers have a right to know when there is reason to believe that their information may have been compromised, and that timely notification in the appropriate circumstances could help to minimize various risks associated with a compromise of customer information. In fact, our actions in this instance actually went beyond the scope of requirements that existed at that time.

Furthermore, our approach and existing policies and practices also are in accordance with the recently issued Interagency Guidance. We believe this guidance strikes the correct balance with respect to when notification is appropriate and what steps should be taken when a security breach has put a customer's personal information at risk. We also believe that a national approach to information security guidelines will promote the most consistent and efficient path to ensuring customer information privacy is maintained.

As the legislative process moves forward to determine the appropriate protections for consumers, we firmly believe it should support the following principles:

- Any business dealing with a customer's personal information has a duty to take all necessary steps to ensure the safety and privacy of that information is maintained.
- Consumers should be notified in a timely manner about any incident that could reasonably lead to the unauthorized use of their confidential information.
- Customer accounts should be monitored for fraudulent activity upon discovery of a potential security breach.
- Institutions and law enforcement must be permitted the opportunity to conduct appropriate investigations in advance of any notice.
- Institutions should protect their customers from any adverse impact from an incident and assist those who are adversely impacted with their recovery.

We believe these general principles are manifested in our actions and they are principles by which we will abide in the future. Our relationship with our customers is built on trust and our actions must always be guided by that bond.

We believe public-private partnerships to advance the cause of information security in this country are critical. We have always maintained that both government and industry have a role to play. We have actively participated in such partnerships and leveraged these working relationships over the past several years with extremely positive results.

In our experience, the best solutions often arise out of the work we do together, implemented through the voluntary cooperation of private sector organizations. The information security environment is by its very nature fluid and rapidly evolving, and demands solutions and counter-measures that can evolve and advance with speed and flexibility.

We look forward to helping promote that speed and flexibility and to taking part in the ensuing legislative dialogue. We also appreciate opportunities such as my appearance before the committee today to share our experience and opinions on such an important matter to our country, its financial systems and consumers.

Members of the committee, on behalf of our leadership team and all Bank of America associates, I can assure you that we will do all we can to make certain that our customers have the freedom to engage in business and commerce and manage their financial lives secure in the knowledge that their personal information will be respected and protected by the institutions in which they place their trust.

This concludes my prepared testimony. I will be happy to answer any questions.