Testimony of Don McGuffey
Vice President, ChoicePoint, Inc.
Before the Senate Committee on Banking, Housing and Urban Affairs
March 10, 2005

Chairman Shelby, Senator Sarbanes and Members of the Committee:

Good afternoon. I am Don McGuffey, Vice President of Choicepoint for Data Acquisition and Strategy. I have been with the company since its inception in 1997.

The Committee has convened this hearing to address the important issues of identity theft and the security of sensitive consumer information. At ChoicePoint, our mission statement recognizes that in an increasingly risky world, information, through the use of modern technology, can be utilized to help create a safer more secure society. We also recognize the risks of inappropriate information use as well as the limitations of technology. We know, and have been painfully reminded by recent events, that there can be negative consequences to the improper use of sensitive personally identifiable data.

As a company committed to the highest standards of information security, we recognize that with respect to the recent events in Los Angeles we failed to prevent certain consumer data from being accessed by criminals. For this we apologize again to those consumers who have been put potentially at risk by this fraudulent activity, and we have and are taking steps to protect them from actual financial harm. We are also actively working with law enforcement to bring to justice those individuals who committed this crime, and we have and will take actions designed to prevent similar violations from occurring in the future.

The modern crime of identity theft, whether in the form of credit card fraud, false business identifications or in its other guises, poses a significant threat to all Americans and we support this Committee's efforts to address that danger. In my testimony today, I would like to tell the Committee about ChoicePoint, describe for you the recent crime perpetrated in Los Angeles, tell you about the steps we have taken to protect individuals who may have been placed at financial risk as a result of this crime and what we are doing to diminish the likelihood of such incidents from occurring in the future. For example, we announced last Friday that our company will discontinue the sale of information products that contain sensitive consumer data except where there is a specific consumer-driven transaction or benefit or where the product supports federal, state or local government and criminal justice purposes.

Mr. Chairman, ChoicePoint is a leading provider of identification and credential verification services to businesses, government, and non-profit organizations. We have approximately 5,000 associates in nearly 60 locations. ChoicePoint provides services to more than 7000 federal, state and local law enforcement agencies, as well as a significant number of Fortune 500 companies, more than 700 insurance companies and many large financial services companies. Our goal is to put the positive power of information to work for society at large. We at ChoicePoint are proud of the company's efforts to identify over 11,000 undisclosed felons among those volunteering or seeking to volunteer with organizations such as the Boys and Girls Clubs of America and of our role in helping law enforcement in numerous instances including our assistance in identifying the DC-area sniper.

Financial and identity fraud is a rapidly growing and costly threat to our nation's economy. ChoicePoint offers a wide range of tools to help avoid fraud but no one is immune from it, as other companies and institutions are also learning. This was underscored by recent events in California, which I would like to describe in more detail to the Committee. On September 27, 2004, a ChoicePoint employee became suspicious while credentialing a prospective small business customer based in the Los Angeles area. This employee brought his concerns regarding the application to the ChoicePoint Security Services Department. After a preliminary review, the manager of the Security Services Department alerted the Los Angeles County Sheriff's Department. They decided to initiate an official police investigation and asked for our assistance. That investigation is still ongoing, and has so far resulted in the arrest and conviction of at least one individual. As we did in the recent Los Angeles incident, we have worked with law enforcement on other occasions of suspicious activity related to customer use of our information products. With respect to California, we have learned that those involved had previously opened ChoicePoint accounts by presenting fraudulently obtained California businesses licenses and fraudulent documents. They were then able to access information products primarily containing the following information: consumer names, current and former addresses, social security numbers, drivers license numbers, certain other public record information such as bankruptcies, liens and judgments and in certain cases credit reports.

Based on information currently available, we estimate that data from approximately 145,000 consumers may have been accessed as a result of unauthorized access to our information products. Nearly one quarter of those consumers are California residents. Since July 2003, California is the only state that statutorily requires affected consumers to be notified of a potential breach of personally identifiable information and authorizes law enforcement officials to delay notification to allow a criminal investigation to proceed. Last fall, we received such a request from the Los Angeles County Sheriff's Department after the issue of consumer notification was discussed between ChoicePoint and the Department. At that time ChoicePoint had not yet reconstructed all of the searches required to identify consumers at risk and law enforcement officers had not learned all pertinent details of the crime. Working cooperatively with the Sheriff's Department and after completing the necessary reconstruction, we began the process of notifying consumers last month. We elected to utilize the California law as the basis for notifying consumers in all states. Absent specific notification from law enforcement personnel, affected consumers or others, we can not determine whether a particular consumer has been a victim of actual identity theft. However, law enforcement officials have informed us that they have identified approximately 750 consumers nationwide where some attempt was made to compromise their identity.

Mr. Chairman, our efforts to protect affected individuals did not stop simply with notification in California. We notified consumers nationwide and have taken other steps to assist potentially affected consumers who we have identified to date. These include:

- providing dedicated toll-free customer service numbers and a special web site to respond to inquiries and to provide information associated with the tools for which ChoicePoint has paid;
- purchasing and providing free of charge a combined 3-bureau credit report; and
- purchasing and providing free of charge a one year credit monitoring service.

We hope our efforts will help those individuals take steps to protect their personal data from being used in a criminal manner.

In addition, we have taken steps to minimize the likelihood of future occurrences of this nature:

- We have decided to exit the non-FCRA consumer sensitive data market, meaning we will no longer sell information products containing sensitive consumer data including social security and drivers license numbers except where there is a specific consumer driven transaction or benefit or where the products support federal, state or local government and criminal justice purposes. We will continue to provide authentication, fraud prevention and other tools to large, accredited corporate customers where consumers have existing relationships.
- We have strengthened our customer credentialing procedures and have embarked on a re-credentialing process for certain customer segments, including all small business customers.

- We have created an independent Office of Credentialing, Compliance and Privacy that will report to the Board of Directors' Privacy Committee. This office will oversee improvements in customer credentialing processes, the expansion of a site visit based verification program, and implementation of procedures designed to expedite the reporting of future incidents. This office will be led by Carol DiBattiste, the Deputy Administrator of the Transportation Security Agency and a senior former prosecutor in the Department of Justice with extensive experience in the detection and prosecution of financial fraud.
- We have also appointed Robert McConnell, a 28-year veteran of the U.S. Secret Service and former chief of the federal government's Nigerian Organized Crime Task Force, to serve as our liaison to law enforcement officials.

Chairman Shelby, to conclude we have all witnessed the significant benefits to society that can come with the proper use of information. ChoicePoint is proud of the role it has played in assisting law enforcement and intelligence agencies as well as vast segments of the American business community in preventing fraud. We have also learned first-hand the damage that can be caused when criminals improperly obtain access to consumer information. We have spoken out previously and would welcome a broad national debate on these issues and support efforts by the Congress to provide for independent oversight and increased accountability of entities that handle public record data. We also support increased penalties for theft of personally identifiable information and a reasonable nationwide mandatory notification requirement of any unauthorized access to personal data. As I noted previously, we determined that our commitment to consumers required us to go beyond both the geographic and substantive requirements of existing law and therefore provided nationwide notification and various consumer protection services for those affected. As Congress continues its work in this area, we stand ready as a company to cooperate with your efforts and look forward to participating in the continued discussion of issues related to identity theft and the protection of sensitive consumer information.

I would be pleased to answer any questions that you might have.