Testimony of

Oliver I. Ireland

On Behalf of the

American **Bankers** Association

Before the

Senate Banking Committee

United States Senate

On

Identity Theft

September 22, 2005

Mr. Chairman and Members of the Committee, my name is Oliver Ireland. I am a partner in the law firm of Morrison & Foerster LLP, practicing in the firm's Washington, D.C. office. I am here today on behalf of the American Bankers Association (ABA) to address the role of banking institutions in protecting consumers from identity (ID) theft and account fraud.

ABA, on behalf of the more than two million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership—which includes community, regional, and money center banks and holding companies, as well as savings associations, trust companies, and savings banks—makes ABA the largest banking trade association in the country.

In general terms, ID theft occurs when a criminal uses personal identifying information relating to another person (generally, a name, address, and Social Security number (SSN)) to open a new account in that person's name. ID theft can range from using a person's personal identifying information to obtain a cell phone, lease an apartment, open a credit card account, or obtain a mortgage loan or even a driver's license. In addition, in some

cases, information relating to consumer accounts can be used to initiate unauthorized charges to those accounts.

The issue of ID theft and account fraud, and related concerns about data security, are of paramount importance to banking institutions and the customers that we serve. ID theft and account fraud can harm consumers and banking institutions, and challenge law enforcement. A major priority of the banking industry is stopping ID theft and account fraud before it occurs, and resolving those unfortunate cases that do occur. Both consumers and banking institutions benefit from a financial system that protects sensitive information relating to consumers, while remaining efficient, reliable, and convenient.

In my statement, I would like to emphasize three key points:

I. Banking Institutions Are Already Regulated

Unlike many other industries that maintain or process consumer information, banking institutions and their customer information security programs are subject to regulatory requirements and regular examinations. Banking institutions have a vested interest in protecting sensitive information relating to their customers, and work aggressively to do so.

II. Uniform Approach Will Promote Information Security

The security of sensitive consumer information will be promoted most effectively by a uniform national standard.

III. Security Breach Notification Requirements Should be Risk-Based

Any requirements should focus on situations that create a substantial risk of identity theft. Over-notification of consumers about breaches of information security will desensitize consumers and may lead consumers to ignore the very notices that explain the action they need to take to protect themselves from ID theft.

I. Banking Institutions Are Already Regulated

Among those that handle and process sensitive consumer information, banking institutions are among the most highly regulated and closely supervised. Title V of the Gramm-Leach-Bliley Act (GLB Act), and associated rulemakings and guidance, require bank institutions not only to limit the disclosure of customer information, but also to protect that information from unauthorized accesses or uses and to notify customers when there is a breach of security with respect to sensitive information relating to those customers.

Banking institutions have a strong interest in protecting customer information. Banking institutions that fail to earn and to maintain the trust of their customers will lose those customers. In the competitive market for financial services, consumers tend to hold their banking institution accountable for any problems that they experience with their accounts or information, regardless of the actual source of the problem. For example, if fraud is committed on a bank account as a result of a breach of security at a data processor working for a retailer—an entity that the bank does not control—the customer is likely to first seek a solution through his or her bank. Therefore, information security is critical in order for banking institutions to maintain customer relations.

Because banking institutions do not impose the losses for fraudulent accounts on consumers and because banking institutions do not impose the losses associated with fraudulent transactions made on existing accounts on their customers, banking institutions incur significant costs from ID theft and account fraud. These costs are in the form of direct dollar losses from credit that will not be repaid, and also can be in the form of indirect costs, including reputational harm. In addition, when a breach of information security occurs at a banking institution, the banking institution typically incurs other costs in responding to that breach. Accordingly, banking institutions aggressively protect sensitive information relating to their customers.

Existing Security Guidance

Earlier this year, the federal banking agencies revised their guidance, originally issued in 2001 under Section 501(b) of the GLB Act, concerning the security of customer information. The revised guidance requires banking institutions to notify their customers of

breaches of the security of sensitive information relating to those customers. We support the agencies' action and recommend their general approach as a model for going forward.

Already in force, the guidance requires banking institutions to establish and maintain comprehensive information security programs to identify and assess the risks to customer information and then to address these potential risks by adopting appropriate security measures. The guidance requires that each banking institution's program for information security must be risk-based. Each banking institution must tailor its information security program to the specific characteristics of its business, customer information, and customer information systems, and must continuously assess the threats to its customer information and customer information systems. As those threats change, a banking institution must appropriately adjust or upgrade its security measures to respond to those threats.

A banking institution must consider access controls on its customer information systems, background checks for employees with responsibilities for access to customer information systems, and a response program in the event of unauthorized access to customer information. Not only do these requirements apply to customer information while in the banking institution's customer information systems, the guidance also requires that a banking institution's contracts with its service providers must require those service providers to implement appropriate measures to protect against unauthorized access to or use of customer information.

A banking institution also must implement a risk-based response program to address instances of unauthorized access to customer information. A risk-based response program must include plans to:

- Assess the nature and scope of an incident of unauthorized access to customer information, and identify what customer information systems and the types of customer information that have been accessed or misused;

- Notify the banking institution's primary federal regulator "as soon as possible" about any threats "to sensitive customer information;"

- Consistent with Suspicious Activity Report (SAR) regulations, notify appropriate law enforcement authorities and file SARs in situations involving federal criminal violations requiring immediate attention; and

- Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information. This could include, for example, monitoring, freezing, or closing accounts, while preserving records and other evidence.

Existing Notification Requirements

A critical component of the guidance is customer notification. The guidance dictates that when a banking institution becomes aware of a breach of "sensitive customer information," it must conduct a reasonable investigation to determine whether the information has been or will be misused. If the banking institution determines that misuse of the information "has occurred or is reasonably possible," it must notify, as soon as possible, those customers to whom the information relates. Customer notification may be delayed if law enforcement determines that notification will interfere with an investigation and provides a written request for a delay. The banking institution need only notify customers affected by the breach where it is able to identify those affected. If it cannot identify those affected, it should notify all customers in the group if it determines that misuse of the information is reasonably possible.

The customer notification standards established by the guidance combine tough security measures with practical steps designed to help consumers. These standards assure a timely, coordinated response that enables consumers to take steps to protect themselves, in addition to knowing the steps that their banking institution has taken to address the incident. The guidance permits banking institutions to focus their resources in a result-orientated way, without requiring unnecessary and possibly misleading customer notifications.

The customer notices required under these standards must be clear and conspicuous. The notices must describe the incident in general and the type of customer information affected. In addition, the notices must generally describe the banking institution's actions to

protect the information from further unauthorized access and include a telephone number by which the customers can contact the institution concerning the incident. The notices should remind customers to remain vigilant over the following 12 to 24 months and to promptly report incidents of suspected ID theft to the institution. Where appropriate, the notices also should include:

- Recommendations that the customer review account statements immediately and report any suspicious activity;

- A description of fraud alerts available under the Fair Credit Reporting Act (FCRA), and how to place them;

- Recommendations that the customer periodically obtain credit reports and have incorrect information removed from those reports;

- Explanations of how to obtain a free credit report; and

- Further information about the agencies' guidance.

Risk-Based Standard

The agencies' approach encourages banking institutions to work on an ongoing basis with their regulators and customers, while requiring the institutions to take concrete and well-defined steps to address a suspected security breach. Immediately upon the discovery of a breach of any size or scope, banking institutions are required to communicate the problem to their primary regulator and to begin devising a strategy to best deal with the problem. This fosters close cooperation between banking institutions and their regulators in order to keep the focus where it belongs: protecting consumers.

Although serious, a data security breach does not automatically, nor necessarily, result in ID theft or account fraud. Customer data is stored and transmitted in a variety of unique media forms that require highly specialized and often proprietary technology to read, and may be subject to sophisticated encryption. Even if customer data finds itself in the wrong hands, it is often not in a readable or useable form. Banking institutions and their regulators need to

retain the ability to react to each situation using a risk-based approach, which takes into account the ability to use the information to harm consumers through identity theft or account fraud.

II. Uniform Approach Will Promote Information Security

In order to provide meaningful and consistent protection for all consumers, all entities that handle sensitive consumer information - not just banking institutions – should be subject to similar information security standards. For example, retailers, data brokers, and even employers collect sensitive consumer information, but many of these entities are not subject to data security and/or security breach notification requirements. These entities, including data brokers, such as ChoicePoint, universities, hospitals, private businesses, and even the Federal Deposit Insurance Corporation, have been the victims of security breaches. The information security breaches that have occurred at banking institutions over the past year represent only a small percentage of the breaches that have been reported. However, any entity that maintains sensitive consumer information should protect that information and should provide notice to consumers when a security breach has occurred with respect to that information and the affected consumers can take steps to protect themselves.

It is not necessary to design a completely new system to address this issue. The regulations that already apply to banking institutions offer policymakers both a model and a measure of experience to aid in establishing umbrella consumer protections that span all industries that maintain sensitive consumer information. In considering the extension of bank-like regulation to unregulated industries that maintain sensitive consumer information, we believe that Congress should focus on a uniform approach that is designed to protect consumers from actual harm.

Uniformity Benefits Consumers

National uniformity is critical to preserving a fully functioning and efficient national marketplace. A score of state legislatures have already passed new data security or privacy bills that will take effect in 2006. While these laws have many similarities, they also have many differences. Millions of businesses—retailers, insurers, banks, employers, landlords, and others—use consumer information to make important everyday decisions on the

eligibility of consumers for credit, insurance, employment, or other needs. State laws that are inconsistent result in both higher costs and uneven consumer protection. In some cases, a single state that adopts a unique requirement or omits a key provision can effectively nullify the policies of the other states.

III. Security Breach Notification Requirements Should be Risk-Based

While it is important to protect all sensitive consumer information from unauthorized use, it is most critical to protect consumers from ID theft and account fraud. In order to avoid immunizing consumers to notices that information about them may have been compromised, security breach notification requirements, like the federal banking agencies guidance, should be limited to those cases where the consumer needs to act to protect himself or herself from substantial harm. Security breach notification requirements should be tailored to those circumstances and, within these circumstances, to the type of threat presented.

For example, a breach involving consumers' names and SSNs may expose them to the risk of ID theft, while a breach involving account information may pose no risk or cost to the consumer or may require the consumer to follow established procedures to reverse erroneous changes to their accounts. In each case, the need for notification and the form of notification will differ. Any federal legislative requirement must recognize and accommodate these differences.

Other Issues

While we believe that federal legislation should focus on the security of sensitive consumer information and notification where a breach of that security threatens substantial harm to consumers, we recognize that in connection with this debate other issues, including the ability of consumers to place "security freezes" on their credit reports and the regulation of the display or sale of SSNs, have been raised. With respect to security freezes, we believe that the FCRA fraud alert system adopted in the Fair and Accurate Credit Transactions Act of 2003 appropriately alerts creditors to the potential for ID theft on particular accounts. It would be premature to discard this system in favor of a system of security freezes that could significantly disrupt the credit granting process by preventing consumers from obtaining credit without going through time-consuming procedures to lift security freezes.

With respect to potential limitations on the display or sale of SSNs, it is important to avoid unintended consequences. For example, disrupting the many transactions that rely on these numbers, including the identification of bank customers for purposes of Section 326 of the USA PATRIOT Act, could harm consumers and national interests.

Finally, it is important to remember that regulatory compliance costs fall disproportionately on community banks. Any legislative solution to data security must consider these and other costs that would be imposed on community banks and their customers.

Conclusion

Bank institutions are proud of their record in protecting sensitive information relating to their customers, and will continue to work with the Committee and banking regulators to ensure that consumers receive the highest level of protection possible.

Thank you. I will be happy to answer any questions that you may have.