TESTIMONY OF

OLIVER I. IRELAND

ON BEHALF OF THE

FINANCIAL SERVICES COORDINATING COUNCIL

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS

AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

ON

H.R. 3997

THE "FINANCIAL DATA PROTECTION ACT OF 2005"

November 9, 2005

Mr. Chairman and Members of the Subcommittee, my name is Oliver I. 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 Financial Services Coordinating Council, which consists of the American Bankers Association, the American Council of Life Insurers, the American Insurance Association and the Securities Industry Association. Together these associations represent a broad spectrum of financial services providers, including banks, insurance companies and securities firms. Our members have a strong interest in protecting our customers from identity theft and account fraud.

In general terms, identity 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. Identity 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 a person's financial account cannot be used to commit identity theft, but instead the information can be used to commit account fraud, that is, to initiate unauthorized charges to a person's financial account.

The issues of identity theft and account fraud, and related concerns about data security, are of paramount importance to financial institutions and the customers that we serve. Identity theft and account fraud can harm both consumers and financial institutions, and represent a challenge to law enforcement. A major priority of the financial services industry is preventing identity theft and account fraud before they

occur, and resolving those unfortunate cases that do occur. Both consumers and financial institutions benefit from a financial system that protects sensitive information relating to consumers, while remaining efficient, reliable, and convenient.

I would like to emphasize three key points:

I. Financial Institutions Are Already Regulated.

Unlike many other industries that maintain or process sensitive information relating to consumers, financial institutions and their customer information security programs are already subject to regulatory requirements. Further, financial institutions have a vested interest in protecting sensitive information relating to their customers, and work aggressively to do so.

II. A Uniform Approach Will Promote Information Security.

In today's world of nationwide financial markets, identity theft and account fraud do not recognize state boundaries. A consumer victim of identity theft may reside in one state, the identity thief may reside in another state, the financial institution victim of identity theft may be in a third state and the information that enabled the identity thief to perpetrate the crime may have been obtained in a fourth state. In this context, consumers will be most efficiently and effectively served by a uniform national standard applicable across financial services holding companies and to all entities that handle sensitive consumer information.

III. Security Breach Notification Requirements Should be Risk-Based.

Any security breach notification requirement should focus on those situations where a security breach creates a substantial risk of identity theft or account fraud. The alternative would result in over-notification of consumers. Over-notification about breaches of information security likely will needlessly alarm or desensitize consumers. Over-notification may lead consumers to ignore the very notices that explain the action they need to take to protect themselves from identity theft or account fraud or lead them to take unnecessary action in situations where the likelihood of identity theft or fraud may not exist. Notification should focus on situations that may lead to substantial harm to the consumer.

FINANCIAL INSTITUTIONS ARE ALREADY REGULATED

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

Financial institutions must obtain and maintain sensitive personal information in order to serve their existing and prospective customers. Financial institutions have a strong, independent interest in protecting customer information and in having that information protected by third parties. Financial institutions that fail to earn and to

maintain the trust of their customers will lose those customers. Financial institutions have long recognized the importance of maintaining and protecting both the confidentiality and the security of this information and ensuring that it is not compromised.

In the competitive market for financial services, consumers tend to hold their financial institutions accountable for any problems that financial institutions experience with their account or information, regardless of the actual source of the problem. For example, if account fraud is committed as a result of a breach of security at a data processor working for a retailer—an entity that the account-holding financial institution does not control—the customer is likely to first seek a resolution through his or her financial institution. Therefore, information security is critical in order for financial institutions to maintain customer relations.

Financial institutions also are victims of identity theft, just as consumers are. For example, because banks do not impose the losses for fraudulent accounts on consumers and because financial institutions do not impose the losses associated with fraudulent transactions made on existing accounts on their customers, financial institutions incur significant costs from identity theft and account fraud. When a breach of information security occurs at a financial institution, the financial institution typically incurs costs in responding to that breach. Accordingly, financial institutions aggressively protect sensitive information relating to their customers.

Existing Data Security and Security Breach Notification Requirements

The federal banking agencies and the Securities and Exchange Commission have established regulations or guidance covering the security of customer information under section 501(b) of the GLBA. In addition, 34 states have adopted comprehensive regulations or statutes that establish standards for insurance companies with respect to safeguarding customer information. Under the customer information security guidance issued by the federal banking agencies, banks are required to notify their customers of breaches of security of sensitive information relating to those customers.

Going forward, any federal legislation should recognize the existing federal requirements that apply to financial institutions, and avoid subjecting financial institutions to duplicative and potentially inconsistent requirements. Further, federal legislation should recognize that financial institutions often operate in a holding company structure and also recognize the benefits to consumers and financial institutions from the "one-stop shopping" that the holding company structure facilitates. These benefits could be significantly impaired by the imposition of differing requirements on different types of financial institutions within a holding company. A financial services holding company should be able to apply existing and uniform federal requirements for data security and security breach notification to all institutions within the holding company.

In this regard, the state-based regulatory system for insurance companies reflected under the GLBA presents unique challenges. As noted above, 34 states have adopted customer information security requirements under section 501(b) of the GLBA. To date, only one state has adopted security breach notification requirements under that section.

Insurers, like other financial institutions, however, are subject to the non-uniform breach notification laws enacted by some 20 states. Given the critical need for uniformity and harmonization in data security and security breach notification requirements, particularly across financial services holding companies, insurers have no objection to new legislative requirements for data security as proposed in H.R. 3997 for insurers.

Insurers strongly support uniform national standards for the investigation and notice of security breaches and uniform enforcement of these standards. Accordingly, we support enforcement of insurers' compliance by the Department of the Treasury. If this is not possible, we support exclusive enforcement by the insurance authority of an insurer's state of domicile of both the statute and any implementing substantive regulations jointly promulgated by the relevant federal agencies.

A UNIFORM APPROACH WILL PROMOTE INFORMATION SECURITY

Uniform national standards applicable to all financial institutions are critical to providing meaningful and consistent protection for all consumers. All entities that handle sensitive consumer information—not just financial 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. Many of these entities, including data brokers, universities, hospitals, private businesses and even the Federal Deposit Insurance Corporation have been the victims of security breaches. 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 need to take steps to protect themselves from identity theft or account fraud.

Uniformity Benefits Consumers

National uniformity is critical to preserving a fully functioning and efficient national marketplace. A score of state legislatures already have passed new data security laws. While these state 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. The need to track these differences and factor them into a notification program may—particularly for small institutions—make it more difficult for institutions to send notice to consumers promptly. The complexity resulting from differing state requirements may mean that consumers will experience delays in receiving timely notices. Moreover, an individual state requirement or an individual state's failure to recognize a key provision can effectively nullify the policy choices made by other states. Under current state laws, the failure of one state to permit notices to be delayed for law enforcement purposes may frustrate law enforcement efforts in other states. A state with a breach notification requirement that is not risk-based can effectively override the laws of other states that provide for more targeted risk-based notices. Uniform guidelines applicable nationwide will ensure that consumers receive the same protections regardless of where they live.

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 identity theft and account fraud. In order to avoid unnecessarily alarming and 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 provide clear triggers for notice and should be tailored to the circumstances and to the type of threat presented.

For example, a breach involving consumers' names and SSNs may or may not expose those consumers to the risk of identity theft depending on who obtains the information and the circumstances, particularly whether the information is encrypted or otherwise secured so that it is unreadable or unusable. Similarly, a breach involving account number information may pose no risk or cost to the consumer because of an antifraud program used by the consumer's financial institution or may require that the consumer simply follow established procedures to reverse erroneous charges to their accounts. In each case, the need for notification and the form that the notification should take will differ.

The federal banking agencies guidance under section 501(b) of the GLBA adopts a risk-based approach to security breach notification that encourages banking institutions to work with their federal regulators to address any suspected security breach. 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 address that problem. Banking institutions are required to notify customers only where misuse of the information has occurred or is reasonably possible. This approach to security breach notification 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 identity theft or account fraud. Financial institutions store and transmit customer data 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 its way into the wrong hands, the data often is not in a readable or useable form. Like the banking agencies guidance, federal legislation should recognize that the risks associated with each security breach will differ and, as a result, the appropriate response to each breach also will differ. As a result, federal legislation should adopt a risk-based approach to security breach notification, which takes into account the likelihood that the information has or will be used to harm consumers through identity theft or account fraud.

H.R. 3997

We commend the Subcommittee for its leadership role in developing this important legislation. We are pleased that H.R. 3997 clearly intends to provide a uniform national standard for data security and security breach notification and includes a number of other provisions that we believe are appropriate for federal security breach notification legislation. H.R. 3997, which would amend the federal Fair Credit Reporting Act ("FCRA"), applies broadly to virtually all entities that maintain sensitive information about consumers. Further, H.R. 3997 recognizes that financial institutions must comply

with existing GLBA requirements for data security and security breach notification, and attempts to ensure that these requirements are consistent across the financial holding company structure. H.R. 3997 provides for a risk-based notification scheme that does not require unnecessary notices to consumers. In providing for risk-based notices, H.R. 3997 recognizes that encryption and other means of securing consumer information can mitigate the likelihood of substantial harm and also recognizes the differences between breaches that involve information that can lead to identity theft and breaches that involve information that only can be used for account fraud. In addition, H.R. 3997 recognizes that appropriate risk-control systems can mitigate the risks of identity theft and account fraud and, therefore, any need for notification to consumers.

Finally, H.R. 3997 appropriately limits its focus to consumer information security and security breach notification and does not also address other issues, such as the ability of consumers to place "security freezes" on their credit reports and the regulation of the sale, display or use of SSNs.

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 that certain consumers may be at risk for identity theft. It would be premature to discard this fraud system, which only recently became effective, 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 remove or temporarily lift security freezes.

With respect to potential limitations on the sale, display or use of SSNs, it is important to avoid unintended consequences. For example, disrupting the many

transactions that rely on these numbers, including the underwriting of and paying claims under insurance policies and the identification of bank customers for purposes of section 326 of the USA PATRIOT Act, could harm consumers and national interests.

Finally, while we believe that H.R. 3997 is an important step towards resolving the problem of security of information about consumers, some issues raised by H.R. 3997 still require further resolution. For example, the harmonization provisions for GLBA section 501(b) rules may inadvertently leave the statute open to interpretation that the state insurance authorities may (or are even directed to) promulgate rules under GLBA section 501(b) relating to data security and investigation and notification of security breaches, inadvertently jeopardizing the critical goal of national uniform standards. Also, there continues to be some concern relating to the breadth and clarity of the trigger for investigation notices. Details, such as the need for notification to the United States Secret Service for breaches involving only a single consumer, or a few consumers, and clarification as to which insurance authority will be the "appropriate functional regulator" for insurers doing business in 50 states, may suggest a need to modify the current notification language or prompt regulatory attention under the exception authority that is already included in H.R. 3997. In addition, there is concern with the fraud mitigation provisions and the proposed specificity and standardization of notices. Other issues will undoubtedly arise during the legislative process.

Further, it is important to remember that regulatory compliance costs fall disproportionately on smaller financial institutions. Any legislative solution to data security and security breach notification must consider these and other costs that would be imposed on these institutions and their customers.

CONCLUSION

Financial institutions are proud of their record in protecting sensitive information relating to their customers. While we recognize that new regulatory requirements inevitably entail changes to existing practices, however sound, as well as additional costs, we will be pleased to continue to work with the Subcommittee to ensure that information about consumers is protected appropriately.

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