TESTIMONY

OF

IRA D. HAMMERMAN
SENIOR VICE PRESIDENT AND GENERAL COUNSEL
SECURITIES INDUSTRY ASSOCIATION

ON

EXAMINING THE FINANCIAL SERVICES INDUSTRY'S RESPONSIBILITY TO PREVENT IDENTITY THEFT AND PROTECT SENSITIVE CONSUMER FINANCIAL INFORMATION

COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS

UNITED STATES SENATE

SEPTEMBER 22, 2005

The Securities Industry Association[1] (SIA) welcomes the opportunity to testify concerning the financial services industry's responsibility to prevent identity theft and to protect the sensitive financial information of its customers. Maintaining the trust and confidence of our customers is the bedrock of our industry. The long-term success of our markets depends on customers feeling confident that their personal information is secure, and we therefore devote enormous time and resources to the protection of customer data. We are, however, concerned that the expanding patchwork of state – and local – laws affecting data security and notice will make effective compliance very difficult for us and equally confusing for consumers.

[1] The Securities Industry Association brings together the shared interests of approximately 600 securities firms to accomplish common goals. SIA's primary mission is to build and maintain public trust and confidence in the securities markets. SIA members (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. According to the Bureau of Labor Statistics, the U.S. securities industry employs nearly 800,000 individuals, and its personnel manage the accounts of nearly 93-million investors directly and indirectly through corporate, thrift, and pension plans. In 2004, the industry generated $236.7 billion in domestic revenue and an estimated $340 billion in global revenues. (More information about SIA is available at: www.sia.com.)

Data security and notice is the legacy of precedents set by the passage, in 1999, of the Gramm-Leach-Bliley Act ("GLB"), which this Committee was so instrumental in passing. We therefore applaud your leadership, Chairman Shelby, and that of Senator Sarbanes, in holding this hearing today. We are pleased that your Committee, given its breadth of understanding of the financial services industry, is actively reviewing these important data security issues.

As you know, at least four other Congressional Committees – the Senate Commerce Committee, the Senate Judiciary Committee, the House Financial Services Committee, and the House Energy and Commerce Committee – are currently actively involved in drafting legislation addressing many of these same issues, each with the intent to move their bills to the floor.

We are hopeful that, as a result of the review you and your colleagues are embarking upon today, you will agree with the conclusion that we and many others have reached – that the problem of data security, especially in this unique time, is a distinct federal responsibility that requires a targeted federal legislative and regulatory response. In light of the increasing number of disparate federal and state legislative proposals, we urge this Committee to strike the appropriate balance that addresses both the concerns of American consumers threatened by identity theft and the duty of those of us in the financial services industry to provide meaningful protections.

Since 1999, SIA, through its member firm committees and working groups, has addressed the issues surrounding the protection of consumer financial information. During this period, SIA representatives have engaged in a dialogue with the Securities and Exchange Commission ("SEC") staff to discuss the industry's requirements under the privacy provisions of GLB,

including obligations to secure sensitive consumer information. In this regard, an SIA committee, comprised of representatives from 18 broker-dealers, meets regularly to discuss and focus on issues relating to the use, sharing, safeguarding and disposal of personal customer information.

SIA and its membership have identified six fundamental principles that we hope this Committee will consider in drafting data breach legislation. Before turning to them, however, we wish to underscore our considered view that all businesses that have custody of sensitive personal information have a responsibility to provide data security measures commensurate with the sensitivity and nature of the data, and to notify consumers whenever a breach of security creates a significant risk of identity theft to the consumer. All businesses should protect the information that consumers provide to them, and justify the trust those consumers place in them by doing so.

Federal legislation addressing these duties must be carefully targeted to ensure that it is meaningful and can be speedily enacted. Legislation that extends beyond data breach, possibly into unrelated areas of privacy, will inevitably slow down the legislative process and delay, if not lessen, the chances for a prompt and appropriate Congressional response.

OVERVIEW

As the Committee is well aware, Section 502(b) of GLB generally prohibits financial institutions from disclosing "nonpublic personal information" to nonaffiliated third parties without first providing those consumers with an opportunity to "opt out" of such a disclosure. In addition, and even more relevant to the issues being addressed here today, section 501(b) of GLB

specifically requires financial institutions to implement appropriate "administrative, technical, and physical safeguards" designed to protect the security and integrity of their customer information. Congress fully recognized the inherent obligation of financial institutions to protect consumer information when it drafted Title V. To that end, and pursuant to GLB, on June 22, 2000, Regulation S-P was issued by the SEC.[2] This regulation requires every broker-dealer, investment company, and investment adviser registered with the SEC to adopt written policies and procedures designed to institute administrative, technical, and physical safeguards for information pertaining to sensitive customer records and information. In addition, broker-dealers are subject to periodic examination by the SEC and Self-Regulatory Organizations for compliance with Regulation S-P.

Earlier this year, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Office of the Comptroller of the Currency, and the Board of Governors of the Federal Reserve System collectively issued interagency guidance, again pursuant to Title V of the GLB, which sets forth certain affirmative obligations aimed at protecting sensitive financial information and notifying customers in the event of a security breach ("Interagency Guidance").[3]

As the functional regulator for the broker-dealer industry, the SEC is similarly well-situated to issue guidance for broker-dealers, and SIA looks forward to working with this Committee, SEC Chairman Cox and the SEC staff in determining how best to construct a notification regime that considers the likely effect of notification thresholds currently in effect in various state data security breach notification statutes. Specifically, as we discuss in more detail below, we would

[2] 17 C.F.R. Part 48.
[3] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736-54 (Mar. 29, 2005).

urge that the Committee consider a standard that links an obligation to notify consumers in the event of a breach with the crime of identity theft. We are concerned that any notification threshold that the Committee might consider for application to the broker-dealer industry should be tied to an actual threat to the consumer to which he or she might reasonably and effectively be expected to respond, and we believe that functional regulators (like the SEC) are best suited to monitor how industry conforms to statutory requirements.

In considering legislation relating to data breach, SIA believes that the Committee should create a statutory framework under which regulations can properly and effectively be promulgated. In doing so, we urge the Committee to consider the following six principles:

- a clear national standard to achieve a uniform, consistent approach that meets consumer expectations;

- trigger for consumer notice tied to significant risk of harm or injury that might result in identity theft;

- a precise definition of sensitive personal information tied to the risk of identity theft;

- exclusive functional regulator oversight and rulemaking authority;

- flexible notification provisions; and

- reasonable administrative compliance obligations.

PRINCIPLES FOR LEGISLATION

Uniform National Standards

As of this morning, a total of 19 states – and one major metropolitan area, New York City – have passed security breach notification laws, and a number of other states are poised to consider legislation in this area. Very few states provide exceptions to coverage for functionally regulated entities at the federal level. Although much of the early legislation enacted in the states was modeled after California's 2002 security breach notification law, which was the first in the nation, states are increasingly enacting much broader legislation that differs in many respects from the original California law.[4]

For example, New York City enacted three laws in May, marking the first instance of a locality enacting an ordinance placing affirmative obligations on businesses to safeguard data, dispose of it in a secure manner, and notify consumers in the event of a security breach. In addition, New York City also authorized the Commissioner of the New York City Department of Consumer Affairs to "refuse to issue or renew" any business license to any New York City business applicant or licensee if there are, among other things, "two or more criminal convictions within a two-year period of any employees or associates of the applicant or licensee for acts of identity theft or unlawful possession of personal identification information." Additionally, any licensed business must "immediately notify the department upon the occurrence" of a judgment or conviction against any employee, or the business itself, of any one of several enumerated offenses. These laws all went into effect three days ago, on September 19, 2005.

[4] The California legislation, S.B. 1386, was enacted in 2002 and went into effect on July 1, 2003.

Although some of these New York City provisions will likely be preempted by the recently enacted New York State data security breach bill, the provisions authorizing the denial of business licenses may not be preempted due to the construction of the preemption clause in the New York state legislation. The clear implication to regional and national businesses of this law is that, potentially, 100,000 or more localities in the United States may similarly decide to seek passage of their own data security compliance regimes, further complicating the compliance obligations of businesses that operate in more than one locality across the nation. To this point, apart from the California and New York legislation, no other state has specifically incorporated provisions into their legislation preempting local branches of government within their states from instituting their own data security legislation.

From a policy perspective, a patchwork of 19 (and likely more) state laws, let alone those of potentially thousands of localities, does not and will not serve the public interest. In fact, the multiplication of state and local laws is likely to exacerbate the confusion and potential harm to consumers. Consumers in different states would be subject to different security standards and levels of notification despite the fact that the harm they may suffer as a result of a security breach at the same institution is identical. Additionally, businesses would be subject to such an array of obligations, which would be ever-shifting, that they may not be able to comply in one jurisdiction without running afoul of the obligations imposed on them in another.

For these reasons, SIA strongly urges that this Committee act quickly to create and obtain passage by Congress of legislation that results in a uniform national standard without subjecting the industry to a myriad of conflicting state and local laws.

Harm/Injury Trigger For Notice

A principal benefit to uniform national standards is the creation of a consistent definition for a trigger that results in the notification of consumers in the event of security breaches. SIA recommends that the Committee create a statutory framework that defines a reasonable and balanced notification trigger to be activated following a breach of security. Specifically, consumers must be notified when there is a "significant risk" that they will become victims of identity theft.

Under the California breach notification law, for example, the unauthorized acquisition of sensitive information – regardless of whether any harm has or could result from its acquisition – creates an obligation for the custodian of that data to notify consumers that it has been so acquired. The Interagency Guidance issued this year proposed that consumer notifications be issued whenever it was reasonable to expect that the data would be misused in a manner creating substantial harm or inconvenience to a consumer.[5] Of course, companies are always free to unilaterally issue notifications whenever they feel it is appropriate to do so. However, a federal mandate should be linked to some sort of demonstrable risk of harm to the consumer, such as the

[5] In testimony before the Senate Commerce Committee this past June, Federal Trade Commission ("FTC") Chairman Deborah Majoras observed that neither the "unauthorized acquisition" standard of California law nor the "misuse" standard of the Interagency Guidance is optimal. Instead, she and her colleagues on the FTC suggested a different standard, one in which notifications would automatically go to customers when a significant risk of harm to them exists as a result of the breach. *See* Prepared Statement of the FTC before the Committee on Commerce, Science and Transportation on Data Breaches and Identity Theft (June 16, 2005).

possible theft of the consumer's identity. Notification in the wake of each incident of data breach, without regard to significant risk of identity theft that might result, could well have the counterproductive effect of overwhelming customers with notices that bear no relation to significant risk, and therefore might not only needlessly frighten and confuse people, but also likely desensitize them to future notices altogether.

Linking the notice trigger to a significant risk of harm strikes the appropriate balance for both consumers and financial institutions alike. Specifically, before a broker-dealer is required to notify potentially great numbers of customers of a security breach, it should be obligated to make a determination, following a reasonable investigation, that a significant risk of identity theft has occurred or could occur as a result of the breach. SIA recommends that the actual formulation for the notification trigger should be determined by functional regulators, through rulemaking. In the case of broker-dealers, the SEC is in the best position to make that determination.

Precise Definition of Sensitive Personal Information

As noted previously, 19 states and one locality have already passed laws imposing consumer notification requirements in the event of a security breach. In many of these states, the scope of the information covered by the laws varies widely. For example, Arkansas and Delaware have expanded California's definition of "personal information" to include medical information, while the definitions in the Illinois and Maine statutes include account numbers, regardless of whether they are accompanied by the security code required to access the account.

New York State's recently enacted law expands the definition of covered personal information even further, to include "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person," when acquired in combination with a social security number, driver's license or state identification number, or account number with a password or access code. Additionally, New York City's ordinance covers all forms of data, whether on paper or computerized, and whether encrypted or not. In addition, the North Carolina legislature unanimously passed a law just last month, which now awaits only the governor's signature, that would specifically cover "personal information in any form (whether computerized, paper, or otherwise)". This raises a question as to whether oral statements containing personal information are also covered by the impending North Carolina data security and notification law.

SIA believes that the scope of the type of information that underpins any notification obligation should be carefully defined so that the obligation to notify only arises when the sensitive personal information acquired in the breach can actually be used to perpetrate the crime of identity theft upon a consumer. For instance, in the absence of a key, encrypted information is useless to others who acquire it and should be excluded from the definition of sensitive personal information, as it was in the California law. Consumers would benefit more from a specific definition of covered personal information which includes combinations of identifying data, as opposed to a broad definition that includes any single piece of information which could not alone be used to steal a consumer's identity.

Exclusive Functional Regulator Oversight and Rulemaking Authority

Given the existing regulatory framework of GLB and the depth of expertise of the functional regulators in dealing with issues like identity theft and data security, any legislation should continue to recognize the primary role of the functional regulators in addressing these issues by granting them exclusive rulemaking and oversight authority.

Functional regulators are in the best position to evaluate the risks for consumers served by each sector of the financial services industry and to determine the specific consumer protection measures that best address them. Functional regulators also have the expertise to adjust these protections over time as threat levels change and the industry's ability to respond evolves. Likewise, functional regulators have the ability to examine the institutions they regulate for compliance and sanction those not in compliance. Accordingly, legislation addressing the security of data held by securities firms and other financial institutions subject to GLB should provide that the functional regulators of these institutions have the exclusive authority to develop and enforce appropriate regulations.

Flexible Notification

The number and variety of security breaches reported in the press over the past eight months have made clear that the optimal means of notification will vary with the type and scope of security breach.

Accordingly, SIA suggests that businesses should be permitted to deliver the customer notice in any timely manner designed to ensure that a customer can be reasonably expected to receive it.

The specific requirements of any notification process should be determined by the functional regulators whose unique expertise will allow them to determine the optimal means of notification.

Reasonable Compliance Obligations

Security breaches may occur through no fault of the business and despite the existence of reasonable safeguarding measures. As Deborah Majoras, Chairman of the FTC, said when she testified before the Senate Commerce Committee this past June, "It is important to note…that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." When that happens, businesses should be permitted to raise as an affirmative defense that they have acted in good faith and implemented systems to reasonably comply with applicable regulations. This opportunity will create incentives for businesses to better secure data and reward those who have already taken such steps.

SIA supports a compliance regime that is both reasonable and predictable, with appropriate administrative liability for those businesses that fail to take the appropriate measures to protect sensitive consumer information. Given the complexity of the issues surrounding a data breach, and the intimate knowledge that functional regulators have about the financial services industry, SIA believes that any bill the Committee drafts should provide for administrative enforcement only.

CONCLUSION

American consumers and industries are currently facing a major threat from criminals, including potential terrorists, who seek to perpetrate identity theft. The financial services industry takes very seriously its duty to safeguard the sensitive financial information that pertains to its customers. The damage created by incidents of identity theft and other kinds of fraud are not only attacks on consumers, but of serious concern to businesses whose reputations inevitably suffer from security breaches and who must bear the cost of the fraud in both lost customers and reduced confidence in their brand.

We believe that to resolve these issues, the Banking Committee should work to create carefully-targeted legislation that embodies the principles we have outlined above. SIA is eager to serve as a valued resource for the Committee in this endeavor, and welcomes the opportunity to work with the Committee and its staff as it continues this critically important work.

Mr. Chairman, thank you again for the opportunity to testify before the Banking Committee today. I welcome your questions, and those of your colleagues, and will endeavor to answer them fully and completely.