Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

Prepared Statement of

Mark Bohannon
General Counsel & Senior Vice President

Software & Information Industry Association (SIIA)

HR 3997,

The "Financial Data Protection Act of 2005"

Before the
Subcommittee on Financial Institutions
And Consumer Credit

U.S. House of Representatives

November 9, 2005

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

PREPARED STATEMENT

Mr. Chairman, members of the Subcommittee, I appreciate this opportunity to appear before you today and testify on the fundamental need to establish a national framework for data security, including effective and meaningful security plans and breach notification.

As the principal trade association of the software and digital information industry,[1] SIIA was one of the first voices urging federal action to address the myriad of state laws that have emerged since California's first went into effect in 2003. We are working with all relevant Committees on both sides of the Capitol to accomplish this objective.

In our view, a national framework should be premised on the track record of the "Safeguards Rule" under the Gramm-Leach-Bliley Act, which many Members and staff of this Committee were instrumental in constructing. As both a comprehensive, yet adaptable model, the "Safeguards Rule" emphasizes on-going security plans to combat the pernicious effects of identity theft, giving consumers uniform protection that can be effectively enforced by authorities and implemented efficiently by business. Within this existing framework, notification is one additional tool – but not the silver bullet – that can advance the goals of the Safeguards Rule.

Our review of HR 3997 is premised on two considerations: (1) While some of our members are regulated as "financial institutions" under existing laws, most of SIIA's members are software companies, ebusinesses, and information service companies, as well as electronics companies, that are subject to the jurisdiction of the Federal Trade Commission (FTC) and its Section 5 authority. It is the effect of HR 3997 on these companies that we ask the Committee to consider as the bill moves through the process. (2) We review each legislative proposal through a set of principles that we believe are central to a meaningful national framework.

In a number of respects, it is clear that the goals and objectives of HR 3997 are consistent with these general principles, some of which we highlight below. While we believe that there are important improvements that can be made to make the bill more workable and effective,[2] we urge the Committee to continue its work on this bill and to work with other relevant Committees to ensure that a coherent national approach is achieved in this Congress.

---

[1] The more than 700 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

[2] We will be providing the Committee with more detailed suggestions following the hearing.

For example, HR 3997 shares one of our key principles: to create a meaningful national data protection framework. With more than twenty-one (21) states having already enacted data security and breach notification laws (most in this current calendar year), a national standard is needed to avoid confusion to consumers, businesses and the appropriate enforcement authorities. We believe the bill can be improved by streamlining the obligations on data security policies and procedures along the lines of the existing "Safeguards" provisions of GLBA so as not to over proscribe the steps and requirements an entity must take. We also appreciate the changes made to HR 3997, prior to introduction, to clarify the roles of 3rd parties in the event of breaches. However, we would suggest further clarification that notices – in order to be effective and ensure consumer awareness and responsiveness – must come from the entity with whom the consumer has the direct relationship, while permitting, as the bill does, the allocation of costs and logistical responsibilities through contracts.

On the critical issue of establishing a meaningful threshold for breach notification, there is a growing consensus to avoid over-notification to consumers. In testimony before Congress, four of the five FTC Commissioners, including the Chair, urged that the meaningful standard should be where a breach "creates a significant risk of identity theft." Our review of HR 3997 finds that the bill includes several thresholds. Taken together, these are likely to lead to confusion. Confusion leads to over notification. To avoid this result, as well as avoid consumer frustration and the possibility of unintended consequences (like increased incidences of phishing as a result of notification), SIIA strongly urges that:

- the threshold should be clearly established upfront and be based on the reasonable belief of an entity that owns or maintains sensitive financial personal information that a breach of such data in electronic form has occurred and there is a significant risk of identify theft; and

- the bill should specify that where data is collected, maintained or used with established information security practices, such as encryption, access controls, redaction or truncation, no such significant risk exists. This approach both facilitates the adoption of good practices, while not over proscribing the means to get there.

In discussions with all Committees, SIIA has recommended clear instructions to regulators, including the FTC, not to impose technology mandates. Virtually every proposal now before Congress has recognized this need, and we hope the Committee will include a similar provision in HR 3997. This language should not preclude steps to encourage voluntary adoption of security best practices.

Central to an effective national framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. We continue to review how the definition of "sensitive financial personal information" that includes both sensitive *financial account* information and sensitive *financial identity* information will in practice work. We note that "identity" information includes some items (such as taxpayer ID number) that are generally available and used regularly in commerce. As such, we urge the Committee to narrow the items included in the definition.

We also strongly recommend that the definition of sensitive financial identity information exclude information that is otherwise available from public sources. It is impractical and unworkable to require businesses to be held liable when the data is publicly available (whether over the Internet or from government offices or libraries). From the consumer perspective, there is little benefit in being notified where the information is otherwise available from public sources. We note for the Committee that the vast majority of states (18) that have adopted laws have included exceptions for publicly available information.

SIIA commends the bill for taking steps to avoid unnecessary or frivolous litigation by vesting "exclusive" responsibility for enforcement with the agencies of functional jurisdiction. To avoid the very real risk of unnecessary litigation, we urge that the legislation recognize that private rights of action or class actions that are premised in whole or in part upon the defendant violating any provision of the bill are counterproductive and should be precluded.

HR 3997 utilizes the enforcement framework of the Fair Credit Reporting Act. As a consumer protection statute, SIIA supports full enforcement of the FCRA, and many of our members supported the amendments made in the last Congress by the Fair and Accurate Credit Transaction Act (FACTA).

As a means for establishing an enforceable national framework on data breaches and notifications, we believe the following should be considered by the Committee:

First, most SIIA members are already subject either to the FTC's enforcement authority under Section 5, which builds on the "Safeguards Rule" of the Gramm-Leach-Bliley Act, or in some limited cases, to the provisions of the GLBA. Through cases brought under Section 5, the FTC has found a variety of unfair and deceptive practices ranging from failure to implement appropriate information security programs[3] to deceptive security claims made by companies.[4]

[3] *BJ's Wholesale*, (FTC Docket No. 042 3160)(June 16, 2005).

[4] See *Petco Animal Supplies, Inc.* (FTC Docket No. C-4133) (Mar. 4, 2005); *MTS Inc., d/b/a TowerRecords/Books/Video* (FTC Docket No. C-4110) (May 28, 2004); *Guess?, Inc.* (FTC Docket No. C-4091) (July 30, 2003); *Microsoft Corp.* (FTC Docket No. C-4069) (Dec. 20, 2002); *Eli Lilly & Co.* (FTC Docket No. C-4047) (May 8, 2002). Documents related to these enforcement actions are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.)

However, HR 3997 leaves companies that are already subject to Section 5 enforcement open to duplicative and even contradictory requirements.[5] As we read HR 3997, nothing in the bill addresses this potentially confusing enforcement situation.

Second, HR 3997 defines a "financial institution" as any company that maintains the social security numbers of its employees or maintains a taxpayer ID number of its customers. We are deeply concerned that this definition extends the concept of "financial institution" well beyond any that has been used to date, and potentially brings a wide range of companies under the FCRA in a manner that was not anticipated when the FCRA was enacted or updated.[6]

In addition, the definition of "consumer report" has been changed to include any report "bearing on a consumer's …personal identifiers…" and therefore subject to the FCRA. While it remains unclear what "bearing on" implies, there is great concern that the practical effect of this change is to cause any business disseminating information that contains "personal identifiers" -- an undefined term in HR 3997 -- to potentially be regulated as a consumer reporting agency under the FCRA regardless of how commonplace those identifiers are. Those businesses could find their ability to sell common products using common "identifiers" -- such as alumni directories or "who's who" directories -- to be restricted to only those buyers with a permissible purpose under the FCRA, a change that would have a catastrophic effect on those businesses.

Third, we share the bill's goal of effectively preempting state laws by having a national framework supersede any state or local requirements. At the same time, we are cognizant that case law is emerging on the *scope* of federal prerogatives in this area, even where tightly written language on preemption has been incorporated, as appears to have been done in HR 3997.

For example, the Ninth Circuit in this area "generally presume[s] that Congress *has not intended* to preempt state law, starting `with the assumption that the historic police powers of the States [are] not to be superseded by [federal legislation] unless that is the clear and manifest purpose of Congress.'"[7] In determining whether the specific preemption provisions of the FCRA supersede California Senate Bill 1 – which is directly targeted at financial information – the analysis of the federal courts in the 9th Circuit rests on whether the information "fall[s] within the scope of information governed by the FCRA" and whether the information is for a "FCRA authorized purpose."[8]

---

[5] HR 3997 includes provisions designed to avoid duplication with GLBA, and our more detailed comments to HR 3997, which we will submit after the hearing, includes suggestions to improve these particular provisions.

[6] At the same time, we note that a "financial institution" *as currently defined* is exempted from the requirements of HR 3997

[7] *ABA v. Lockyer*, Docket No. CV-04-00778-MCE (9th Circuit), decided June 20, 2005, citing *Cipollone v. Liggett Group, Inc.*, 505 516 (1992) (internal brackets, citation, and quotation marks omitted in original).

[8] ABA v. Lockyer, E.D.Calf., decided on remand from the 9th Circuit, October 6, 2005.

To date, no state enacting a data breach notification law (including those with safeguards provisions) has limited the scope of its law to the financial sector or to specifically regulated information. This is especially true of the first such state law enacted in California. SIIA looks forward to working with the Committee to achieve the shared goal of enacting a meaningful national framework that avoids courts having the last word on whether federal law preempts state laws in this area.

Mr. Chairman, to ensure that a coherent policy approach is achieved by Congress, we once again urge this Committee to continue its work on this bill and to work with other relevant Committees as the process unfolds. We appreciate the opportunity to appear before you today. I will be glad to take any questions that you might have.