Statement of the U.S. Chamber of Commerce

ON: **"THE FINANCIAL DATA PROTECTION ACT"**

TO: **HOUSE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT**

BY: **KARL F. KAUFMANN**

DATE: **NOVEMBER 9, 2005**

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

STATEMENT OF KARL F. KAUFMANN
SIDLEY AUSTIN BROWN & WOOD LLP
ON BEHALF OF THE UNITED STATES CHAMBER OF COMMERCE

Hearing on H.R. 3997, the Financial Data Protection Act
Before the Subcommittee on Financial Institutions and Consumer Credit

November 9, 2005

Good morning Chairman Bachus, Ranking Member Sanders, and members of the Subcommittee. My name is Karl Kaufmann and I am an attorney in the Washington, DC office of the law firm Sidley Austin Brown & Wood LLP. I am pleased to appear before you this morning on behalf of the United States Chamber of Commerce. The Chamber is the world's largest business federation, representing more than 3 million businesses of every size and in every sector of the economy.

In General

Mr. Chairman, the Chamber supports your effort, and the efforts of others on the Subcommittee, to develop legislation to protect the sensitive information of consumers. This morning I intend to discuss some of the key themes important to the Chamber with respect to data security and consumer protection. First, Congress should require that companies have reasonable programs to safeguard consumers' sensitive personal information, similar to the requirements imposed on financial institutions under the Gramm-Leach-Bliley Act ("GLBA"). Second, we believe it is appropriate for a company, upon discovery of a data breach, to notify consumers if their sensitive personal information has been acquired by an unauthorized person in a manner that presents a significant risk of harm to the consumers. If Congress decides to require additional consumer remedies in the wake of a data breach, we strongly urge Congress to recognize the different types of information that can be compromised and the different types of harm that can result. The Chamber also urges Congress to review the criminal penalties associated with hacking to determine whether additional penalties are necessary to deter and punish those who seek to obtain sensitive consumer information. Finally, and perhaps most importantly, any law passed by Congress must establish a national uniform standard with respect to information security, customer notification, and other related issues. This national uniform standard should be enforced solely by the appropriate federal agencies.

In general, the Chamber believes that H.R. 3997, the Financial Data Protection Act, approaches the above principles in a reasonable manner and therefore provides a sound framework for development of stronger consumer protection. We also understand that the legislation continues to evolve and that it may require additional refinement. We applaud you and the bill sponsors for establishing an open process to receive feedback from all interested parties, a process that began during the early developmental phases of the legislation. Such a constructive process has the potential to result in legislation which can gather broad support. The Chamber looks forward to continuing to work with you,

Mr. Chairman, and others to continue to shape this complex bill as it moves through the legislative process.

Information Security

Protecting consumers sensitive personal information is a priority for companies holding such information. We believe that the vast majority of companies who possess sensitive personal information take reasonable procedures to safeguard that information. There are strong market forces in place to encourage companies to protect information because the reputational and economic harms associated with a data breach can be severe. However, it takes only a few mistakes by a few companies to damage consumer confidence in the ability of all companies to protect sensitive information. Therefore, we believe it is appropriate to require companies that possess sensitive personal information to have reasonable procedures in place to protect the integrity and security of such information.

The Chamber believes that the information security requirements established under the GLBA for financial institutions should serve as a blueprint for the requirements that should apply to other companies that possess sensitive personal information. In this regard, the GLBA standards provide financial institutions with a risk-based approach to information security, requiring that programs be appropriate to the company's size, complexity, and activities. The Chamber believes that the information security requirements included in H.R. 3997 establish a data protection regime that takes a risk-based approach, recognizing that a "one size fits all" solution for companies of varying sizes and complexity is inappropriate. We commend the sponsors of H.R. 3997 for establishing such a framework and urge that this approach be retained.

Consumer Notification

Although companies implement reasonable security programs, and H.R. 3997 mandates such programs, there is no such thing as the "perfect" security program. Unfortunately, there will be occasions on which unauthorized individuals obtain sensitive information about consumers. We believe that consumers should be notified of certain security breaches in order to take appropriate steps to protect themselves from harm.

There are several issues which must be decided in connection with notifying individuals about security breaches. For example, what is a "security breach"? Such a definition is critical because it sets the baseline of circumstances for when consumer notices may be required. If the definition is too broad, consumers may receive notices when they are not necessary. If it is too narrow, consumers may not receive notices when they would be appropriate. The Chamber believes that a security breach in the context of the legislation is an event when an unauthorized individual acquires sensitive consumer information. This is similar to how H.R. 3997 defines a security breach.[1]

[1] We note that the legislative definition also includes "an unusual pattern of use of [sensitive consumer] information indicative of financial fraud." This prong of the definition may cause unintended

Although the definition of a security breach is important, it is not the only factor in determining whether a consumer should be notified of the breach. A critical factor is whether or not the breach, once discovered, is likely to result in substantial harm to an affected consumer. Only when the consumer is at risk for substantial harm will such a notice have true meaning to the consumer. For example, if a phone book publisher realizes that crates of undelivered phone books were stolen from its warehouse, it does not seem reasonable that the publisher should notify each of the consumers listed in the phone book of the "breach". This example is illustrative for two reasons. First, the information—name, address, and phone number—is not sensitive insofar as it is not of the type that would allow someone to commit fraud in the individual's name. Second, even if name and address were sufficient to commit fraud, the breach itself is unlikely to be the cause of substantial harm to the consumer because the phone books are available virtually anywhere. As a result, to "notify" consumers that the information in the phone book has been breached would be entirely unnecessary. Moreover, if consumers tend to receive notices of technical "breaches" that do not pose significant risks to consumers, such as a notice describing a breach at the phone book publisher, consumers may begin to ignore security breach notices. If this occurs, the goal of using consumer notices to inform the consumer of the breach, the consumer's rights, and how the consumer can protect him or herself is defeated.

Therefore, if we are to protect consumers properly, it is absolutely critical that consumers receive notices only when: (i) sensitive information is breached; and (ii) the breach is likely to result in substantial harm to consumers. If breach notices are limited to these circumstances, in the unfortunate instance when a consumer receives such a notice, it is much more likely that the consumer will be aware that the notice is important and should be read closely. The sponsors of H.R. 3997 appear to agree with the Chamber's view on this key issue. The trigger in the legislation is designed to ensure that notices are sent to consumers only when they would be meaningful, a concept the Chamber strongly supports.

We believe that there are several factors that should be taken into account when determining whether a consumer is at risk of substantial harm as a result of a breach. For example, very sensitive information could "fall into the wrong hands," yet if the information is protected by strong encryption the consumer is unlikely to be at risk of any harm at all. In fact, the Chamber would support efforts to deem the unauthorized access of encrypted information as unworthy of consumer notice, similar to an approach taken in California and other states. At the very least, data encryption should be a factor in determining whether the consumer may be harmed as the result of a breach. We also agree with H.R. 3997 that certain circumstances simply do not rise to level of requiring a notice, such as if a credit card account is closed and the card is reissued.

Mitigation of Harm

---

consequences, as many entities have programs to detect unusual patterns of information usage which are not indicative of a data breach.

The legislation requires companies to provide consumers with free access to credit file monitoring services for a period of time in certain circumstances. In particular, if the consumer is at risk of becoming a victim of identity theft as a result of a security breach, the breached entity must make available free credit file monitoring services for six months. Although consumers who are potential identity theft victims could access their credit report up to six times a year at no charge under current law, we believe that additional statutory mitigation may prove appropriate under the limited circumstances specified in the legislation. In particular, the Chamber is pleased that the bill distinguishes situations in which consumers may become victims of identity theft, and therefore may have reason to monitor their credit file, from situations where consumers may become victims of credit card account fraud for example. Although we fully recognize the impact of fraud on consumers and others, credit file monitoring is not a tool used to remedy credit card account fraud. In this regard, misuse of a credit card account without misuse of the accountholder's identification information will not be reflected on the consumer's credit file. Rather, if the transaction is not blocked by anti-fraud networks, the consumer would be alerted of the fraud via the periodic credit card statement. Of course, the major credit card companies voluntarily provide zero liability for those fraudulent transactions.

National Uniformity

The Chamber believes it is imperative for Congress to establish a set of national uniform standards pertaining to data security and related issues. This is an absolutely essential consumer protection, and we applaud its inclusion in the Financial Data Protection Act. Today there are approximately 20 different states that have laws relating to consumer notification of data breaches. The number of state laws is certain to increase within the next few months.

The proliferation of similar, but ultimately different, state laws with respect to information security issues is not in consumers' best interests. Varying notification standards can result in consumer confusion and inconsistent compliance with the law. Furthermore, the net result is that the states that require notices in the most circumstances will dictate national policy with respect to data breach notification requirements. Companies that operate on a nationwide basis cannot efficiently develop 50 different data breach notification compliance plans in addition to a federal plan. Such companies are likely develop a compliance plan that complies with the most onerous state laws, even if it results in "overcompliance" by sending more notices than required in the majority of other states. This result undermines one of the fundamental concepts included in H.R. 3997, that consumers receive notices only when they are meaningful. The result may also undermine the will of the majority of state legislatures that sought to limit unnecessary notices, but were "overruled" by a minority of states that pursued a different, and flawed, policy objective. We do not believe these types of outcomes are best for consumers. We also believe Congress is in a better position to establish national policy on this inherently interstate issue.

If there is to be a national uniform standard, there must be a national uniform interpretation of that standard. The Chamber is pleased that the Financial Data Protection Act is enforceable solely through administrative enforcement by the appropriate federal agencies. A federal law subject to interpretation by state enforcement agencies or trial attorneys is not truly a national uniform standard.

Deterring Computer Crimes

We believe that the criminals who obtain sensitive personal information in an unauthorized manner should be deterred from their crimes and punished severely. Therefore, the Chamber strongly endorses efforts to provide more resources and tools to law enforcement to investigate and prosecute data security crimes. We endorse increasing the appropriate criminal penalties, both to deter and to punish those who attempt to hack into a computer system. We believe a key component of protecting consumers is ensuring that law enforcement is properly engaged, even if the hacker's attempts were thwarted by strong data security programs.

Conclusion

The Chamber strongly supports many of the concepts addressed in H.R. 3997, the Financial Data Protection Act. We believe that, if properly implemented, these concepts will result in stronger consumer protections. In particular, it is important that companies that possess sensitive consumer information implement reasonable procedures to protect that information. In the event of a security breach which is likely to result in substantial harm to the consumer, affected consumers should receive appropriate notices. In order to ensure consumers receive the appropriate protections, Congress should establish a national uniform standard with respect to issues relating to H.R. 3997. The Chamber recognizes that the Financial Data Protection Act is still subject to further discussion. Mr. Chairman, we look forward to working with you and others to improve H.R. 3997 as it moves through the legislative process. Given the complexity of the legislation, it is extremely important that the legislative language reflect the true congressional intent. Thank you for the opportunity to testify this morning, and I would be happy to answer any questions.