

Statement of Mr. H. Randy Lively, Jr.

CEO and President of the American Financial Services Association.

Testimony Before the House Financial Services Committee

November 9, 2005

Chairman Oxley, Ranking Member Frank and Members of the Committee,

I am H. Randy Lively, Jr., the CEO and President of the American Financial Services Association located here in Washington, DC. It is my honor and pleasure to be here this morning to testify in support of HR 3997, the Financial Data Protection Act of 2005, introduced by Representatives LaTourette and Hooley and cosponsored by a broad bipartisan array of Members of this distinguished committee.

The American Financial Services Association represents the nation's market rate lenders providing access to credit for millions of Americans. AFSA's 300 member companies include consumer and commercial finance companies, "captive" auto finance companies, credit card issuers, mortgage lenders and other financial service firms that lend to consumers and small businesses. I am proud to say that next year, AFSA will celebrate its 90th birthday as the nation's premiere consumer and commercial credit association.

As I mentioned at the outset, I am pleased to be here this morning to speak in support of the Financial Data Protection Act and ask you, Mr. Chairman, to have the committee give it expedited consideration. AFSA and its members believe that well informed, proactive consumers are our best defense and our first line of attack in protecting all of us from the dangers of identity theft.

According to the Federal Trade Commission, identity theft robs the nation of more than \$50 billion annually. Consumer losses account for about \$5 billion of the total and business absorbs the remaining \$45 billion. Yet in addition to the immediate monetary loss suffered, AFSA companies are more concerned about losing the trust of treasured customers, and mishandling a security breach can cost us valued customers.

Obviously, the best way to protect our customers' information is to prevent a security breach from occurring in the first instance. Toward that end, we are focusing on training our own employees in the handling of sensitive personal information, and are scrutinizing the practices of third-party vendors who store or dispose of data which may contain personal financial information. There is no doubt that the industry needs to regularly upgrade and improve the practices and procedures of our own companies and our storage and disposal vendors to prevent security breaches from ever occurring in the first place.

AFSA member companies share this committee's goal of wanting to ensure American consumers that their personal information is safely protected. To accomplish this goal, AFSA members are regularly improving their security measures and procedures to prevent threats to their information systems. HR 3997 provides a clear and concise framework for AFSA's member companies and other financial service providers to follow in the unfortunate event of a data breach.

The authors of the Financial Data Protection Act of 2005 clearly understand that an effective breach notification and reaction system must be based on the real risk to the customer and the businesses that rely on the integrity of the data. If the breach notification system is overly broad

we run the risk of inundating our customers with notices and having them ignore important information they need to protect themselves.

HR 3997 establishes a reasonable and balanced approach for businesses and regulators to prevent potential breaches of data security as well as uniform procedures to follow if one does occur. The legislation appropriately anticipates that some breaches may pose a significant risk of harm or inconvenience to consumers' identities, whereas others may not create a significant risk for the consumer. This distinction will enable businesses to maximize their vigilance over consumer data, apply law enforcement and regulatory resources where they are most needed and focus consumers' attention to take steps to protect themselves when they are truly at risk.

The Financial Data Protection Act of 2005 calls on business to conduct an immediate investigation if it is learned that a breach has occurred to assess the nature and scope of the breach. The investigation will determine whether the breach has created a substantial risk for the customers' personal financial information. The determination will take into account what information has been exposed and whether the information was encrypted, redacted or requires technology that is not commercially available. AFSA believes that the committee should direct the functional regulators to treat the breach of encrypted information as not creating a potential substantial harm unless an actual harm can be demonstrated. In other words, there should be a presumption that the acquisition of encrypted information does not create a substantial risk for consumers to whom the information relates.

Should a business determine that a substantial breach has occurred, HR 3997 directs a company to notify the Secret Service and the appropriate functional regulators as well as third parties that might be affected by the breach. This type of coordinated framework will ensure that ongoing law enforcement investigations are not compromised by premature publication of breaches. At the same time, the legislation provides reasonable parameters so that a delay in notifying consumers does not unnecessarily extend their exposure to risk of harm.

HR 3997 directs that breach notices to consumers must be done in a clear and conspicuous manner that describes the nature of the breach, when the breach occurred, the relationship between the consumer and the entity who suffered the breach, and actions that the business is taking to restore the security and confidentiality of the breached information. The bill also requires that the consumer notice includes a summary of rights the consumer has as a victim of fraud or identity theft. AFSA supports this approach because the legislation also recognizes that a notice that follows this format should only have to be given once.

AFSA whole heartedly agrees with the sponsors of HR 3997 in directing federal regulators to work together to create uniform security standards and policies for each business to implement and maintain to protect sensitive information. Moreover, a uniform national standard replacing the patchwork of varied and numerous state and local requirements will avoid needless duplication that could lead to confusion and divert resources from the actual problem.

I appreciate the opportunity to be here today and would be happy to answer any questions you may have.