



1120 Connecticut Avenue, NW  
Washington, DC 20036

1-800-BANKERS  
www.aba.com

## Memo

*World-Class Solutions,  
Leadership & Advocacy  
Since 1875*

Date: May 24, 2006

To: Members of the House Judiciary Committee

From: Floyd E. Stoner, Executive Director, Congressional Relations & Public Policy

RE: Markup of Data Security Legislation

I am writing on behalf of the members of the American Bankers Association (ABA) regarding H.R. 5318, the Cyber-Security Enhancement and Consumer Data Protection Act, and H.R. 4127, the Data Accountability and Trust Act, which will be considered by the Judiciary Committee on Thursday, May 25, 2006.

The ABA supports uniform national standards for notification to individuals whose personal information has been put at risk by a breach of security, and we commend you for the work you are doing in this important area. Financial institutions are under constant attack by those who want to break into our systems and misuse sensitive personal information about our customers. In that regard, we have experienced increasingly sophisticated attempts at “phishing” to steal customer account information, as well as rising involvement by organized crime.

That is why we strongly support provisions in H.R. 5318 that would make “cyber extortion” a crime, add computer crimes to the list of predicate offenses for purposes of the Racketeer Influenced and Corrupt Organizations (RICO) law, and make federal crimes of unauthorized access to a computer to obtain personal information and the use of “botnets” to access a computer without authorization.

However, we do have continuing concerns about how Section 7 of the bill would be implemented. This section would impose criminal sanctions on institutions that fail to disclose a “major breach” to law enforcement agencies. Although such a provision might be necessary for other types of institutions, financial institutions are already required by law and regulation to inform our regulators immediately in the event of a security breach. There are significant administrative penalties for failing to do so, including heavy monetary fines. Since financial institutions are so heavily regulated, we are very concerned about duplicative regulation and enforcement by other agencies of the federal government. We look forward to working with the Committee to address this concern as the legislative process moves forward.

We would also like you to know that the ABA has serious concerns about H.R. 4127, the Data Accountability and Trust Act, which was referred to the Judiciary Committee from the Energy & Commerce Committee. H.R. 4127 fails to recognize explicitly the stringent Gramm-Leach-Bliley Act (GLBA) standards that are already in place for financial institutions, and instead leaves it to the subjective judgment of the Federal Trade Commission (FTC) to determine whether financial institutions should be subject to both the GLBA and to this new law and additional regulators.

We have several other concerns about H.R. 4127:

- It does not fully preempt state law because it explicitly does not preempt enforcement of “any state consumer protection law” or any law related to “fraud.” These exceptions raise serious concerns that business entities will be subject to both federal and state law, which undermines the goal of having a nationwide standard.
- It authorizes the FTC and the state attorneys general to enforce the data protection and notice requirements of the bill without an exception for financial institutions. This is unnecessary, since financial institutions are already subject to extensive oversight, enforcement, and penalties, including “cease and desist” orders, monetary penalties, and other sanctions by federal and state regulators for violations of the law covering data breaches.
- The definition of “breach of security” is overly broad and will result in expensive and counterproductive over-notification that will provide little if any benefit to consumers. Moreover, the definition of “information broker” is unclear because it may include third-party agents that act as data processors, thereby subjecting them to the sweeping responsibilities imposed by the bill.

Congress should establish a uniform national standard that both recognizes existing law in this area and ensures that consumers receive the same information no matter where they live. We will continue to work with the Committee and others in Congress to address our concerns about H.R. 4127.

Thank you for considering our views on these important issues.