

September 29, 2009

The Honorable Henry Waxman
Chairman
House Committee on Energy and Commerce
Washington, DC 20515

The Honorable Joe Barton
Ranking Member
House Committee on Energy and Commerce
Washington, DC 20515

Dear Chairman Waxman and Ranking Member Barton:

Our members support uniform national standards for notification to individuals whose personal information has been put at risk by a breach of security. However, we continue to have serious concerns about the Data Accountability and Trust Act (H.R. 2221), which will be marked up by the Committee on September 30.

In particular, we are concerned that this legislation will lead to uneven protection for consumers, duplicative requirements for the financial services industry, and exposure to overlapping enforcement agencies. Accordingly, we request that the legislation be amended to expressly exempt financial institutions that are subject to the requirements of Title V of the Gramm-Leach-Bliley Act (GLBA).

We very much appreciate the fact that Commerce Subcommittee Chairman Bobby Rush and other Members of the Committee have made it very clear that there is no intent to impose duplicative regulation on financial services entities that are already required to comply with federal and state data protection and consumer notice requirements. However, we continue to have concerns that H.R. 2221 establishes an entirely new set of rules for dealing with data security and applies them to a broad range of business entities, including financial institutions that are already subject to the data security requirements of the GLBA and other federal and state laws. These concerns were outlined in the attached memorandum sent to your staff on July 9, 2009.

We urge you to address the concerns reflected in the memorandum as the Committee prepares to markup H.R. 2221. Thank you for considering our views on this important issue.

Sincerely,

American Bankers Association
American Council of Life Insurers
American Insurance Association
Independent Community Bankers of America
Securities Industry and Financial Markets Association
The Financial Services Roundtable

Cc: Members of the Energy and Commerce Committee

Attachment

July 9, 2009

To: House Energy and Commerce Committee Staff

From: The Financial Services Industry

Re: H.R. 2221

Thank you for meeting with us on June 30, 2009 to discuss the “Data Accountability and Trust Act” (H.R. 2221) as reported by the Commerce, Trade and Consumer Protection Subcommittee on June 3. Our members support uniform national standards for notification to individuals whose personal information has been put at risk by a breach of security. However we have serious concerns that this legislation will lead to uneven protection for consumers, duplicative requirements for the financial services industry and exposure to overlapping enforcement agencies. Accordingly, we request that the legislation be amended to expressly exempt financial institutions that are subject to the requirements of Title V of the Gramm-Leach-Bliley Act (“GLBA”). As you requested, the following is our analysis of the bill that addresses the reasons for our concerns.

New Requirements for Financial Institutions

We very much appreciate the fact that Chairman Rush and others on the Subcommittee have made it very clear that there is no intent to impose duplicative regulation on financial services entities that are already required to comply federal and state data protection and consumer notice requirements. However, H.R. 2221 establishes an entirely new set of rules for dealing with data security and applies them to a broad range of business entities, including financial institutions that are already subject to the data security requirements of the GLBA and other federal and state laws.

No Explicit GLBA Exception

Sections 2 and 3 of the bill are free-standing provisions that apply to all business organizations, including financial institutions. Section 2(a)(3) of the bill 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 the new data security provisions. Moreover, the bill does not provide any exclusion for financial institutions from the data breach requirements of Section 3. The bill’s failure to explicitly recognize that financial institutions are currently subject to stringent GLBA as well as state and federal standards already in place is, in our judgment, a major flaw.¹

¹ Although many businesses are not subject to a clear legal and regulatory system that requires them to protect consumers’ sensitive personal information, the institutions we represent – the banking, securities, and insurance industries – are already subject to the comprehensive privacy and data security requirements of the GLBA, implementing regulations and extensive supervisory guidance. Title V of the GLBA and its implementing regulations require financial institutions not only to limit the disclosure of customer information, but also to protect that

Duplication in Enforcement

The reason that an explicit exception for financial institutions subject to Title V of the GLBA is critical is that the bill as presently drafted runs the risk that banks, securities firms, insurers, and their subsidiaries and affiliates could be subject to duplicative and perhaps inconsistent regulation and enforcement. Moreover, although Section 18(f) of the Federal Trade Commission Act states clearly that the FTC does not have jurisdiction over a “bank, savings association or credit union”, the Commission has taken an aggressive stance with respect to jurisdiction over bank subsidiaries and affiliates. Therefore, even if an assumption is made that a bank, savings association or credit union are not covered by the enforcement language in Section 4 of the bill, subsidiaries and affiliates of these institutions would potentially not be exempt from FTC regulation and enforcement.

Another reason for an exemption for financial institutions can be found in Section 4(b) of the bill, which authorizes state Attorneys General to enforce the data protection and notice requirements of the bill with respect to financial institutions. Such an enforcement mechanism is unnecessary since financial institutions are already subject to extensive oversight, including “cease and desist” orders, monetary penalties, and other sanctions by federal and state regulators for violations of the law. Enforcement of GLBA data protection and consumer notice requirements should remain exclusively with the primary functional regulators and not state Attorneys General. Accordingly, we urge the Committee to exempt financial institutions that are subject to Title V of the GLBA.

State Law Preemption

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. A patchwork of state notification laws that results in duplicative requirements and uneven consumer protections will not serve our members’ customers or our national financial services system. Because our members serve customers throughout the U.S., it is of vital importance to financial institutions to be able to adopt uniform data security and notification standards that will apply to all consumers on a nationwide basis. The proposed legislation does not satisfy this objective because it does not fully preempt state law or regulations. The bill seeks to establish a national standard, but it explicitly protects state enforcement of “any State consumer protection law” and does not preempt any state law related to “fraud.” Such broad exceptions raise serious concerns that consumers will be subject to uneven protections and business entities will be subject to both federal and state law, undermining the goal of a uniform nationwide standard.

information from unauthorized accesses or uses and, in the case of banking institutions, to notify customers when there is a breach of security with respect to sensitive information relating to those customers. These requirements have been established, and are enforced, by various “functional” regulators at the federal and state levels, including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, the Securities and Exchange Commission, and state insurance authorities.

Accordingly, because of the legislation's failure to provide a uniform pre-emptive standard, we believe that financial institutions subject to Title V of the GLBA should not be covered by H.R. 2221.

Information Broker A further example of our concern with including financial institutions within the scope of coverage of the bill is the overly inclusive definition of the term "information broker." This definition in Section 5(6) of the bill tries to address concerns raised over whether affiliates within holding companies that handle centralized data bases for use by those holding companies fall within that definition. However, concerns continue to exist with this language, including whether third-party agents that act in the same capacity would remain within the definition, thus subjecting them to the sweeping responsibilities imposed by the bill on such brokers.

Conclusion

Therefore, the undersigned organizations urge you to address the concerns reflected in this memorandum as the Committee prepares to markup H.R. 2221. Thank you for considering our views on this important issue.

American Bankers Association

American Council of Life Insurers

American Insurance Association

Consumer Bankers Association

The Financial Services Roundtable

Independent Community Bankers of America

Securities Industry and Financial Markets Association