



Financial Services Coordinating Council

*American Bankers Association • American Council of Life Insurers • American Insurance Association
Securities Industry and Financial Markets Association*

October 15, 2007

The Honorable Bart Gordon
Chairman
House Science and Technology Committee
United States House of Representatives
2320 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Gordon:

The Financial Services Coordinating Council (FSCC) thanks you for the opportunity to participate in your recent roundtable regarding the development of security standards, security testing, security management, and best practices for the protection of data and transactions. The FSCC, whose members are the American Bankers Association, American Council of Life Insurers, American Insurance Association, and Securities Industry and Financial Markets Association, represents thousands of large and small banks, insurance companies, and securities firms that, taken together, provide financial services to virtually every household in America.

During the roundtable, you expressed your concern regarding the growing problems related to data security breaches, a concern that FSCC members share. Regardless of where a particular data breach may occur, a bank, securities, or insurance customer can ultimately be impacted. It is for this reason that the FSCC has advocated that companies outside of the financial services industry be held to the same data security standards that are currently in existence for financial institutions.

You have asked for comment on a number of areas regarding data security, including:

- The need for consensus standards related to protection of data;
- The need for best-practices for protection of data, transactional data and data management;
- An appropriate role for the National Institute of Standards and Technology (NIST) in working in such areas;
- A need for additional research in the area of technology development to better protect data and prevent data breaches;
- The need for programs to educate children and adults about best-practices to prevent against data breach; and
- The need for reasonable enforcement mechanisms for ensuring use of protection technologies and best-practices.

The following are our preliminary thoughts on these issues.

Consensus Standards, Best Practices and Role of NIST

We agree that consensus standards can be helpful. The reality is that several consensus standards and best practices already exist. For instance, the financial services industry has long been a leader in safeguarding customer information, and the regulatory requirements in place for our industry could serve as a model for other industries. Financial services companies are required to safeguard customer information, and can be subjected to enforcement actions if they fail to do so. Federal depository institution regulations also require customer education programs be developed. This broad structure of regulation, education, and enforcement for safeguarding customer information simply does not exist in other industries.

Collaborative standards, in many cases, can be beneficial in assisting financial institutions in meeting their regulatory requirements. Many such standards are cited by financial institution regulators as a resource. Financial institution regulators, however, do not look for absolute compliance with one particular standard or another. Rather, these various standards provide benchmarks that both financial institutions and their regulators draw upon for the development of industry expectations and security practices. Such an approach gives institutions the flexibility to evaluate which standards are most appropriate for their institution, based upon their perceived risk.

While NIST has an excellent record of developing data security standards, other organizations, such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), and the Information Systems Audit and Control Association (ISACA) also have played valuable, collaborative roles in developing such standards. Credit and debit card account data protection standards have also recently been developed on a collaborative basis by the PCI Security Standards Council.

While there are a number of current consensus data security standards and best-practices, gaps can certainly exist. An evaluation of where gaps in standards exist and whether a standard would provide greater levels of data security would be an appropriate role for NIST. FSCC does not, however, recommend giving one standard setting body preeminence over other bodies that have developed very useful resources in the past.

On a related point any effort by the Committee to enhance the role of NIST in the development of data security standards should not be at the expense of or conflict with other standards. Conflicting standards, especially if they have enforcement mechanisms, can pose real dangers for companies.

Technology Research

The Committee has asked whether there is a need for additional research in the area of technological development to better protect data and prevent data breaches. While additional research in this area can prove valuable, care must be taken to ensure that

technology developed out of such NIST efforts does not become a standard that companies must adhere to.

Financial institution regulation regarding safeguarding customer information is risk-based, and given that risks continually change, financial institution regulators take a technologically-neutral approach to regulation and examination. The technology that lies behind a data security standard must have a high degree of flexibility in order to be relevant.

Consortiums providing data security research on a collaborative basis already exist within the financial services industry. For instance, the Financial Services Technology Consortium (FSTC) is a partnership of banks, financial services technology providers, national laboratories, and universities that sponsors noncompetitive collaborative financial services research. One recent project is designed to enable real-time information sharing on fraud incidents and patterns to improve fraud forecasting, detection and mitigation. Another examines the account opening and funds transfer process to minimize the amount of sensitive personal information exchanged and shared.

Enforcement Mechanisms

The financial services industry is already subject to data security regulation and enforcement by its functional regulators at the federal and state levels. There should also be a data protection enforcement mechanism, to the extent it does not already exist, for companies outside this system.

A case in point is the evolving PCI Data Security Standard (PCI DSS), a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures in the credit and debit card environment. Companies, including financial institutions, are required to be certified as “PCI compliant” in order to participate in the credit and debit card payment system. Companies found not to be in compliance with PCI DSS can be penalized. Enforcing a separate, conflicting NIST standard would pose great risk to companies and impose significant compliance costs on them.

The FSCC, and the undersigned organizations that it represents, welcomes the opportunity to continue to work with the Committee. Thank you for considering our views on this important issue.

American Bankers Association

American Council of Life Insurers

American Insurance Association

Securities Industry and Financial Markets Association