Statement for the Hearing Record

Submitted By

ARMA International

To the

Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
U.S. House of Representatives
Washington, DC
Regarding its Hearing on

H.R. 3997, Financial Data Protection Act of 2005

November 9, 2005

Strong Public Policy is Needed to Protect Financial Data Security

Americans demand security and privacy of their personally identifiable information. The establishment of new systems that allow easy access and transference of personally identifiable data between parties should to be sensitive to personal privacy and grant assurance to Americans that their data will not be misused or end up in the wrong hands.

Incidents of breaches of personally identifiable information are on the rise. A 2003 survey of a one-year period by the Federal Trade Commission revealed that more than 10 million people had experienced identity theft in one form or another.[1] Widely-reported episodes of data breach, such as Bank of America and Lexis-Nexis, serve as lessons to information brokers that the highest level of security is required to ensure that personally identifiable information is not compromised. For these reasons, we appreciate the attention that policymakers are giving to this important issue.

Because of the essential role of effective and appropriate information management in today's economy, ARMA International has a strong interest in issues pertaining to safeguarding consumer information and other personally identifiable information possessed by business and government.

While ARMA International lauds efforts to address incidents of financial data breach, we believe that H.R. 3997 does not adequately address the prevention of data breaches. A records and information management program, dedicated as a written set of policies and procedures for the management of information in the custody of an organization, is just as essential an element of any data safeguard regime as are new technologies designed to enhance data security. Therefore, ARMA respectfully urges that the Subcommittee at a minimum enhance the safeguards provisions of H.R. 3997 by incorporating language into the measure directing that mandated data security policies and procedures be in writing and be made available to all personnel with access to sensitive financial information that the bill is intended to protect.

ARMA International's interest in congressional efforts to protect sensitive consumer information is based on our confidence of the role that a written records and information management program plays in maintaining an information security regime in any organization. A sound records and information management policy, guided by the best practices of the field of records management, can serve as an important tool to achieve the goal of securing personally identifiable financial data and preventing data breach. The application of a records and information management program is based on the goal of preserving the security and integrity of all records in the custody of an organization, protecting such records from unauthorized use, and properly disposing of such information appropriately at the end of a records' life cycle.

Once Congress acts to create an affirmative obligation by covered entities to protect the security of sensitive personally identifiable financial information, ARMA strongly

[1] See Federal Trade Commission Identity Theft Survey Report, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

recommends that any data security safeguards include a written program of policies and procedures designed to guide personnel throughout an organization and ensure that records are properly maintained, accessed and disposed of. A written program will also serve as a benchmark, not only for the organization and its leadership to ensure proper compliance with corporate expectations, but also as a guide for regulatory agencies given the responsibility of ensuring that companies do what they profess to do. Our belief in the role of an appropriate written policy also recognizes that no technology can completely address the human component involved in records management.

ARMA acknowledges that the best practices of records and information management are supported by a compelling business argument. A written program that is communicated throughout an organization provides the best defense for an organization should data breaches occur inconsistent with its own policies. But ARMA also acknowledges that not all organizations endorse the best practices of records and information management without external incentives. Legislation designed to protect financial data from unauthorized breach should also include meaningful sanctions when organizations do not put in place reasonable security measures designed to protect sensitive personal information. ARMA notes that H.R. 3997 contains no provisions that would allow regulatory enforcement agencies to impose sanctions upon bad actors who allow data breach to occur when security standards are lax. As currently written, H.R. 3997 provides no penalty for organizations that willfully or wantonly handle consumer financial information, thereby providing no incentive for a covered entity to ensure that the maximum level of security is maintained when handling information.

Why Records and Information Management is Important for Data Security

Information is among the most valuable commodities of any organization. In the case of organizations that possess, process, and use sensitive consumer information, this information is a part of the organization's strategic business model. As such, these organizations have a significant responsibility to manage and maintain the integrity and security of this information, including the implementation of appropriate safeguards against unauthorized use and the proper disposal of the information.

"Records management" is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.[2]

Of primary importance from a records and information management perspective is ensuring the integrity and security of information. Whatever information management systems are in place must ensure protection of the records and information in these two critical areas. Public sector agencies and private sector entities should not have access to personally identifiable information unless the information is essential to the organization's work. It is important that public and private sector entities identify what

[2] See "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"), p. 3.

information is actually mission critical, who within their organizations should have access to the information, and then ensuring that the information cannot be accessed by unauthorized parties. It is the role of a written information management program that informs all employees within an organization of any routine protocols for business records as well as special protocols for legislatively mandated safeguards.

ARMA notes that a significant risk of identity theft occurs at a point when a given record should be destroyed – and the best practices of records and information management and a record's retention schedule would require not only appropriate measures to ensure destruction, but also the documentation of the destruction or final disposition action.

Within the context of managing the life cycle of any information, assuring that records and information are destroyed appropriately – at the time and in the manner anticipated by the organization's retention and disposition program, and in compliance with any applicable law or regulation – is as important and deserves the same level of attention and stewardship as assuring that the information is properly maintained. The appropriate destruction of a record at the end of its life cycle will assist with efforts to secure personally identifiable information and curb identity theft. The same best practices will safeguard the misappropriation of records stored in electronic format.

Records and information management policies provide a guideline for the creation, use, maintenance, and disposition of a record in the ordinary course of business. An appropriate records and information management program in an organization includes setting policies and standards, assigning responsibility and authorities to particular individuals within an organization, establishing procedures and guidelines, providing a range of services relating to the management and use of records, designing, implementing and administering specialized systems for managing records, and integrating records management into business systems. Records contain information that is a valuable historical resource and an important business asset.[3] "A systematic approach to the management of records is essential for organizations and society to protect and preserve records as evidence of actions. A records management system results in a source of information about business activities that can support subsequent activities and business decisions, as well as ensuring accountability to present and future stakeholders."[4]

A records management policy empowers organizations to conduct business in an orderly, efficient and accountable manner, deliver services in a consistent and equitable manner, support decision making by organizational management, provide continuity in the event of a disaster, and meet legislative and regulatory mandates including archival, audit and oversight activities. A vigorous program will also provide protection and support in litigation including the management of risks associated with the existence of, or lack of, evidence of organizational activity, protect the interests of the organization, support

[3] See "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"), p. 4.
[4] Ibid.

current and future research and development activities, and assist with maintaining organizational memory.[5]

ARMA believes that any security regime for personally identifiable information should include support by senior management of a written records and information management program.[6] This would include the appropriate investment in personnel, training and organization-wide communications. It would also ensure that third party relationships endorse the same safeguards with appropriate means of ensuring compliance.

In today's distributed work environments, a wide variety of individuals create records and must therefore take responsibility to ensure those records are captured, identified and preserved. It is no longer enough to train administrative staff and assume they will make sure the records end up in the records management program. All members of management, employees, contractors, volunteers and other individuals share the responsibility for capturing records so they can be properly managed and secured throughout the length of their required retention period. An appropriate records management program includes a risk assessment program which includes conducting a physical site survey, identifying probable threats to records, including the systems vulnerability to deliberate destructive acts.[7]

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) contained a provision that required the Federal Trade Commission and the various banking regulators to develop a disposal rule for sensitive customer information. This rule may provide a model for businesses in other industry sectors for the appropriate disposal of personally identifiable information. In comments[8] to the disposal rules proposed by the Commission and the various banking regulators, ARMA strongly recommended that an organization's safeguards include a formal, written records and information management program.

About ARMA International

Established in 1956, ARMA International (ARMA) is the non-profit membership organization for the records and information management profession. The 10,000 members of ARMA include records and information managers, imaging specialists, archivists, technologists, legal administrators, librarians, and educators employed by both private and public institutions. Our mission includes providing education, research, and networking opportunities to information management professionals, as well as serving as a resource to public policy makers on matters related to the integrity and importance of records and information.

ARMA serves as a recognized standards developer for the American National Standards Institute (ANSI), participating and contributing toward the development of standards for

---

[5] Ibid.
[6] "Requirements for Managing Electronic Messages as Records," P. 3
[7] "Records Programs: Identifying, Managing, and Recovering Business-Related Records" , p. 4.
[8] ARMA's comments on the disposal rule may be viewed at http://www.ftc.gov/os/comments/disposal/index.htm.

records and information management.[9] ARMA is also a charter member of the information and documentation subcommittee of the International Organization for Standardization (ISO), aiding in the development of its records management standard, ISO 15489.[10]

Records and information management plays an important role in the private and public sectors. In this new century, the most valuable commodity of business is information, often in the form of data bases of essential information required by the service sectors of our economy. The greatest responsibility for organizations will be managing and maintaining the integrity of an ever-growing flow of information, including the establishment of appropriate safeguards for sensitive information and in establishing retention schedules complaint with regulatory and statutory requirements. These challenges call for increased recognition of the role of managing critical information and providing appropriate protections for personally identifiable information. Organizations that embrace information management as being strategic and mission critical will ensure their competitive advantage and remain appropriate stewards of information containing sensitive consumer information. Maintenance of an appropriate records and information security program provides numerous benefits, including efficiency, accessibility, and security.[11]

Conclusion

ARMA International applauds the Subcommittee for examining the issue of securing personally identifiable financial information. ARMA recommends that any effective data security initiative include a vigorous records and information management program, informed by written set of policies and procedures, communicated throughout the organization, and supported by senior management, to help ensure that breaches of security do not take place.

Respectfully submitted,
Cheryl L. Pederson, CRM
President
ARMA International
13725 W. 109th St., Suite 101
Lenexa, KS 66215
800.422.2762/913.341.3808
Fax 913.341.3742

[9] "Managing Recorded Information Assets and Resources: Retention and Disposition Program" may be viewed at http://www.arma.org/standards/public/document_review.cfm?DocID=22.
[10] "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"). ARMA fully supports ISO 15489-1.
[11] "Records Center Operations", p. 1.