Before the
Security and Exchange Commission

In the Matter of
Proposed Amendments to Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information
File Number S7-06-08

COMMENTS OF

ARMA INTERNATIONAL

Summary of Comments and Recommendations

In its Notice of Proposed Rule[1] ("Notice"), the Securities and Exchange Commission ("Commission") is proposing amendments to Regulation S–P, which implements certain provisions of the Gramm-Leach-Bliley Act ("GLBA") and the Fair Credit Reporting Act ("FCRA") for entities regulated by the Commission.

ARMA International (ARMA) is committed to policies and procedures, whether voluntary or part of necessary regulatory regimes, that are informed by the best practices of managing records and information as vital assets of an enterprise, and that are based on standards-based Records and Information Management policies and procedures. Given the realities of a global marketplace, and in particular the marketplace participants subject to the Commission's scrutiny, ARMA further encourages rules and regulations, as well as voluntary policies and procedures that are internationally recognized or sanctioned.

ARMA's mission statement includes engaging policy making activities and encouraging legislative and regulatory bodies to utilize the subject matter expertise of our organization and our membership to help drive greater professionalism and reliability in the management of records and information and to serve as an objective voice for the changing standards and solutions in records management practices around the world. ARMA is available to the Commission relative to its current review of the Safeguards Rule and Disposal Rule.

ARMA strongly recommends that the Commission base the Safeguards Rule[2] and Disposal Rule[3] on standards-based policies and procedures for Records and Information Management ("RIM"). These standards[4] are well developed for enterprise-wide

[1] 73 F.R. 13692 et seq. (March 13, 2008)
[2] 17 CFR 248.30(a)
[3] 17 CFR 248.30(b).
[4] ARMA International has participated in the standard setting efforts of both the American National Standards Institute (ANSI) and the International Organization for Standardization (ISO) relative to Records

application, contemplating the life cycle management of all vital and mission-critical records and information, including personally identifiable information, and safeguarding regimes appropriate to records associated with this information. Throughout these comments, we reference and recommend the specific provisions of the standards applicable to Records and Information Management by the American National Standards Institute (ANSI)[5] and the International Organization for Standardization (ISO)[6].

These ANSI and ISO standards on Records and Information Management enable organizations of all sizes and governance models, including small registered brokers and broker-dealers, to install and operate systematic, managed control of their information assets – recognizing the role of the US market in the global economy and our competitiveness in aligning to standards adopted elsewhere are important talking points.

All classes of information, including personal information, cannot be effectively managed as proposed by the Release without being managed within a broader Records and Information Management program. It is not possible to manage one class of data without doing so within a more coordinated effort. The reliability and competitiveness of the industry cannot be advanced otherwise. Therefore, all elements of the proposed amendments, such as training and auditing, in addition to being informed by a proven standards-based regime, should not be isolated on personal data alone, but should be encouraged to be part of the overall Records and Information Management policies and procedures maintained by a regulated entity.

Therefore, ARMA offers the specific recommends to the text of the Commission's proposed amendments to 17 CFR 248.30.

Relative to paragraph (a) describing an Information Security Program, ARMA recommends the following changes (**recommended text is underlined and in bold text**):

> (1) *General requirements.* Every broker or dealer other than a notice-registered broker or dealer, every investment company, and every investment adviser or transfer agent registered with the Commission, must develop, implement, and maintain a comprehensive information security program. Your program must include written policies and procedures that provide administrative, technical, and physical safeguards for protecting personal

---

and Information Management. The text of these comments reference specific sections of these respective standards.

[5] Several ANSI/ARMA standards have been developed to guide Records and Information Management practices and procedures. A full list is available at www.arma.org/standards/index.cfm.

[6] See "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001 ("ISO 15489-1") See also, ISO/IEC 27001:2005, "Information Technology—Security techniques—Information security management systems—Requirements", and ISO/IEC 27002:2005, "Information technology—Security techniques—Code of practice for information security management".

information, and for responding to unauthorized access to or use of personal information. **Your program must be approved by senior management, communicated across your enterprise, and be supported with adequate training and auditing processes to ensure compliance.** Your program also must be appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any personal information at issue. **In developing and managing your program, you should take account of standards-based Records and Information Management practices and procedures, and your information security program should be integrated with the enterprise-wide programs and procedures for records and information management otherwise required to be maintained.**

(3) *Safeguards*. In order to develop, implement, and maintain your information security program, you must:

(i) Designate in writing an employee or employees to **manage and** coordinate your information security program;

Relative to the written policies, procedures and records under paragraph (b) describing the disposal of personal information, ARMA recommends the following changes (**recommended text is underlined and in bold text**):

(2) *Written policies, procedures and records*. Every broker or dealer, other than a notice-registered broker or dealer, every investment company, and every investment adviser and transfer agent registered with the Commission must:

(i) Adopt written policies and procedures that address the proper disposal of personal information according to the requirements of paragraph (b)(1) of this section; and

(ii) Document in writing its proper disposal of personal information in compliance with paragraph (b)(1) of this section.

Your program must be approved by senior management, communicated across your enterprise, and be supported with adequate training and auditing processes to ensure compliance. In developing and managing your program, you should take account of standards-based Records and Information Management practices and procedures, and your information security program should be integrated with the enterprise-wide programs and procedures for records and information management otherwise required to be maintained.

In the definitions section, ARMA recommends the following changes (**recommended text is underlined and in bold text**):

> (6) *Information security program* means the administrative, technical, **and** physical safeguards you use to **manage the life cycle of a record of personal information, including** access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.
>
> **NEW DEFINITION: (10) *Records and Information Management Program* means a defined process for achieving 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**

I. About ARMA International and the Role of Information Management

ARMA International (ARMA) is the non-profit membership organization for the world's information management profession[7]. The approximately 11,000 members include records managers, archivists, corporate librarians, imaging specialists, legal professionals, IT managers, consultants, and educators, all of whom work in a wide variety of industries, including government, legal, healthcare, financial services, and petroleum in the United States, Canada, and 30-plus other countries.

Information is among the most valuable assets 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 plan. As such, these organizations have significant responsibility to manage and maintain the integrity of this information, including the implementation of appropriate safeguards against unauthorized use and the proper disposal of the information. Safeguards and proper disposal are essential elements of an organization's information retention and disposition program. An organization's disposal of records of information, such as "consumer information" in the instance of the proposed amendments to The Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Guidelines), is informed by policies and procedures developed, implemented and audited by the organization to ensure compliance and credibility in its stewardship of sensitive personally identifiable information and nonpublic personal information.

ARMA is a recognized standards developer within the ANSI Framework, and a full list of the standards developed by ARMA is available at www.arma.org/standards/index.cfm. In addition, ARMA has actively participated in, and endorses the value of, the

[7] For further information, go to: www.arma.org.

International Organization for Standardization (ISO) International Standard, "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"). ARMA was a charter member of ISO Technical Committee ISO/TC 46, Information and documentation, Subcommittee SC 11, Archives/records management. ARMA fully supports ISO 15489-1.[8]

II. The Role of Records and Information Management in Safeguarding Personally Identifiable Information

First and foremost, ARMA recognizes that a properly developed and implemented Records and Information Management program represents an important element of sound business practice. Relevant to the proposed amendments to the Safeguards Rule described in the Notice, ARMA believes that to be effective, the expected Information Security Program must be a comprehensive Records and Information Management Program, empowered and supported by senior management, apply across an enterprise, and be applicable to all records and information vital and mission critical to an organization.

Records and Information Management principles dictate that all relevant business records remain accessible for the duration of a record's life-cycle. The ISO Standard codifies this assertion –

> "Records are created, received and used in the conduct of business activities. To support the continuing conduct of business, comply with the regulatory environment and provide necessary accountability, organizations should create and maintain authentic, reliable and useable records, and protect the integrity of those records for as long as required."[9]

Records and Information Management programs create enterprise-wide, cost-effective processes and procedures for assuring the validity and accessibility of vital records and compliance with voluntary and legally required retention policies.

Records are initially created for the purpose of conducting business, documenting and fulfilling business obligations and facilitating decision-making processes. Businesses have obligations and requirements that affect how they keep their records, independent of the need to demonstrate compliance with statutory or regulatory requirements. By following accepted and proven Records and Information Management practices,

---

[8] The National Archives and Records Administration (NARA), in its statutory responsibilities to assist and provide guidance to Federal agencies in the development and implementation information management regimes, bases its approach to information management on ISO Records Management Standard 15489. See "Ready Access to Essential Evidence: The Strategic Plan of the National Archives and Records Administration (1997-2008) (Revised 2003)", page 14. NARA's strategic plan may be found at: http://www.archives.gov/about_us/strategic_planning_and_reporting/2003_strategic_plan.html.

[9] See ISO 15489-1:2001, Clause 7.1, "Principles of records management programmes".

informed by the applicable standards of ANSI and ISO, records of information can be maintained for integrity and authenticity, as well as for purposes of safeguarding from unauthorized use, access, or disposition.[10]

A Records and Information Management program should govern the practice of both Records and Information Managers and of any person who creates or uses records of information in the course of business activities.

The ISO Standard recognizes the value proposition of records management –

> "Records contain information that is a valuable resource and an important business asset. 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."[11]

The ISO Standard also speaks to the regulatory environment –

> "All organizations need to identify the regulatory environment that affects their activities and requirements to document their activity. The policies and procedures of organizations should reflect the application of the regulatory environment to their business processes. An organization should provide adequate evidence of its compliance with the regulatory environment in the records of its activities."[12]

Several other elements of a Records and Information Management Program that are applicable to the questions raised by the Commission merit attention:

Management Involvement: The importance of executive level support is reflected in ANSI/ARMA and ISO standards related to various aspects of Records and Information Management Programs.

Section 4.0 of ANSI/ARMA 9-2004, "Requirements for Managing Electronic Messages as Records" states: "The executive management of an organization seeking to conform to this standard shall establish, document, maintain**,** and promote policies, procedures, and

---

[10] Likewise, auditing firms and regulatory bodies can rely on the integrity and authenticity of records captured in a properly implemented Records and Information Management program.

[11] See ISO 15489-1:2001, Clause 4, "Benefits of records management".

[12] See ISO 15489-1:2001, Clause 5, "Regulatory environment".

practices for managing electronic messages and electronic messaging systems that ensure the organization's business needs are met."

Section 5.0 of ANSI/ARMA 8-2005, "Retention Management for Records and Information" reinforces the importance of top management support: "The ultimate authority for all decisions relating to retention of records resides with the senior management of the organization."

Section 5.2 of the same standard states: "In addition to the information retention and disposition policy statement, senior management should issue specific directives as necessary to ensure support for the information retention and disposition program."

Clause 6.3 of the ISO Standard recognizes that while all employees in an organization have some responsibility for the manner in which organizations keep their records, the level of responsibility and accountability will vary. The standard states: "Records management responsibilities and authorities should be defined and assigned, and promulgated throughout the organization so that, where a specific need to create and capture records is identified, it should be clear who is responsible for taking the necessary action. These responsibilities should be assigned to all employees of the organization, including records managers, allied information professionals, executives, business unit managers, systems administrators and others who create records".

Clause 6.3(b) adds more detail specific to executives by stating, "[e]xecutives are responsible for supporting the application of records management policies throughout the organization"

Records and Information Management Programs are greatly enhanced and effective when the executives demonstrate active support of its requirements. Likewise, records management programs are greatly weakened if the executive level support falls short of providing needed resources, and making financial allocations to enable comprehensive implementation and monitoring.

Training: As with all policies and procedures, training is an essential element of any Records and Information Management Program.

Section 10 of ANSI/ARMA 9-2004 states: "Organizations should provide an ongoing program of user training to facilitate and achieve effective electronic message management. The policy should be communicated to users so that all users are aware of the intent and boundaries of the policy."

Section 9.2 of ANSI/ARMA 8-2005 also references the importance of ongoing training in the implementation of an organization's retention and disposition program.

Clause 11 of the ISO Standard addresses the need for training within an organization seeking to comply with the standard. It recognizes that the records management training for employees should be customized to their particular responsibilities and accountability within the program.

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 throughout the length of their required retention period.

Communication: Closely related to training, is the necessity of communicating the records management program throughout the organization. This theme is reiterated in

Section 4.0 of ANSI/ARMA 9-2004: "The designated records personnel must ensure that the policy is communicated and implemented throughout the company." The Section also requires that records management policies be published and circulated throughout the organization and that responsibilities for compliance be assigned to every user and each individual with a recordkeeping role, including database administrators and information or network technology support personnel.

Section 9.1 of ANSI/ARMA 8-2005 also references the best practice of establishing a manual or processes and procedures relative to records management that is provided to departments and managers throughout an organization.[13]

Clause 6.1 of the ISO Standard, addressing policy and responsibilities, calls on organizations to "establish, document, maintain and promulgate policies, procedures, and practices for records management to ensure that its business need for evidence, accountability and information about its activities is met."

Clause 6.2 of the ISO Standard requires a records management policy be "communicated and implemented at all levels in the organization" and that the policy "be adopted and endorsed at the highest decision-making level and promulgated throughout the organization".

Monitoring and Auditing: Records and Information Management best practices also require ongoing monitoring and auditing. Section 4.1 of ANSI/ARMA 9-2004 requires

[13] Section 9.1 of ANSI/ARMA 8-2005 further requires that a letter from the chief executive officer of the organization stating the purpose of the information retention and disposition program and the need for compliance with the policy from all departments and staff.

that Records and Information Management programs be "regularly reviewed at designated intervals and revised, as needed, to reflect current compliance requirements.

Section 7.2 of ANSI/ARMA 8-2004 requires that records management policies authorize individuals within the organization to "monitor equipment, systems, electronic message traffic at any time for security and network maintenance purposes" and that the organization retain authority to "audit networks and systems on a periodic basis to ensure policy compliance".

Clause 10 of the ISO Standard calls for regularly undertaken compliance monitoring "to ensure that the records systems procedures and processes are being implemented according to the organizational policies and requirements and meet the anticipated outcomes". It further calls for "modifications" if the records systems and records management processes "are found to be unsuitable or ineffective".

Section 9.3 of ANSI/ARMA 8-2005 states: "Compliance with the information retention and disposition program is the responsibility of the organization and all employees. Employees should be aware of the program and its requirements – especially the effects of inappropriate or premature disposition of records…Compliance with the information retention and disposition program should be reviewed on a regular basis, determined by organization policy".

Management of Change: The ANSI/ARMA standards recognize that it is important to document the policies and procedures on which the records management program is based, and that it is important to maintain corporate integrity of the information management environment by periodically assessing the policies, systems and practices that are in place to ensure they are still relevant to a changing business environment. Nearly everything in the information management environment is subject to frequent change (legal requirements, organizational infrastructure, technology, regulations and business process changes).

Clause 6.2 of the ISO Standard indicates that "Policies should be regularly reviewed to ensure that they reflect current business needs". Clause 8.4.(h), addressing post-implementation review, states: "Gather information about the performance of the records system as an integral and ongoing process…. Review and assess the performance of the system, initiate and monitor corrective action and establish a regime of continuous monitoring and regular evaluation."

Retention Periods: The determination of retention periods for various record types within an organization is a complex process involving data gathering, analysis, and decision-making as the basis for the retention and disposition schedule. The various elements of this process are further specified in ARMA International's most recent

standard, "Retention Management for Records and Information" (ANSI/ARMA 8-2005).[14]

Without being comprehensive, the above references should adequately demonstrate that the importance of executive level support, communication, training, change management and auditing and compliance are well recognized in Records and Information Management standards at both the national and international level.

III. The Role of an Information Retention and Disposition Program in the Life Cycle of Information

ARMA has previously commented specifically on the development of rules for proper disposal of personally identifiable information. [15]

During consideration of the FACT Act on the floor of the U.S. Senate, Senator Richard Shelby of Alabama offered Amendment Number 2067, on behalf of Senator Bill Nelson of Florida, to include a new section to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) to require the promulgation of regulations regarding the disposal of consumer credit information. See Cong. Rec. S13889 (Nov. 4, 2003).

In a brief statement included in the Congressional Record by Senator Nelson, the amendment's author noted "that some companies do not have protocols in place outlining the proper way to dispose of private consumer information when it is no longer needed." [emphasis added]

Senator Nelson recounted a specific incident whereby "thousands of files containing sensitive customer records were discarded in a dumpster," noting that the information greatly compromised the individuals whose personally identifiable information was contained in the records to "numerous crimes, including identity theft."

Long recognized in the field of Records and Information Management, the "protocols" referred to by Senator Nelson that outline the proper way to dispose of records and information are articulated in an organization's formal, written information retention and disposition program, a part of its Records and Information Management Program.

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

[14] The ISO Standard devotes the majority of Clause 9 to the analytical process behind analyzing business activities, determining the various uses of the records and determining how long to keep them.

[15] ARMA commented in the proceedings initiated by the Federal Trade Commission relative to the disposal of information as required under the FACT Act: The FACT Act Disposal Rule, Docket No. R-411007, and in the proceedings initiated by the Board of Governors of the Federal Reserve System relative to the disposal of information as required under the FACT Act: The FACT Act Disposal Rule, Docket No. 1199.

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 safeguarded during its retention period – both for the use of an organization in pursuit of its business purposes as well as for safeguarding the information from improper use during the useful life of the information.

A records retention and disposition program is that component of an organization's records management program that defines the period of time during which records are maintained, and specifies procedures for the transfer and disposition of records. The retention and disposition program addresses the period of time the records are in use by the organization, the method of disposal or disposition, and the procedures for ensuring compliance with the program.

The goal of an information retention and disposition program is to ensure that recorded information is identified, appraised, and maintained for an appropriate period of time in such a way that it is accessible and retrievable. It is disposed of at the end of the total retention period. The existence of, and compliance with, an information retention and disposition program is important to meet that goal and to avoid premature disposition, and/or unauthorized disposal or retention, or recorded information.

Of the core elements of an information retention and disposition program that ARMA has recommended in the past are (1) the identification of the retention period for each covered record, (2) the method of disposal or disposition, and (3) procedures for ensuring compliance. This last point will require at a minimum the involvement and approval by senior management, training of employees with responsibility over the covered records, appropriate controls of the disposition and disposal of the covered records, and documentation of all disposition and disposal actions.

ARMA notes that Senator Nelson's observation during the Senate consideration of his amendment included not only the need to articulate the proper way to dispose of information, but to do so "when [the information] is no longer needed." The timing of the disposition of information is an equally important element to the management of records of information and is properly informed by an organization's retention and disposition program, safeguarding the information during its useful and intended life cycle, and ensuring that proper procedures and personnel management are in place to secure proper or required destruction.

ARMA also notes that a properly implemented and audited information and disposition program will provide an important safeguard against the improper disposal of the records as recounted by Senator Nelson. It ensures that an organization's personnel are informed and appropriately trained in the proper retention and disposition procedures and it provides for meaningful oversight of an organization's practices by regulatory agencies with jurisdiction over the custodians of the records and information involved.

ARMA has therefore argued for the importance and effectiveness of a formal, written information retention and disposition program. In our comments regarding the establishment of FACT Act Disposal Rule, ARMA noted that while the text of the Section 216 of the FACT Act does not specifically refer to an organization's adoption of a retention and disposition program, proper disposal and the safeguarding of consumer information during custody, potentially from "cradle to grave" for some organizations, is more properly ensured by such a program. Our comments were further informed by recognized practices of documenting the disposal of information and records.

ISO 15489-1, Clause 8.3.7, "Retention and disposition", provides: "Records systems should be capable of facilitating and implementing decisions on the retention and disposition of records.[16] It should be possible for these decisions to be made at any time in the existence of records, including during the design stage of records systems. It should also be possible, where appropriate, for disposition to be activated automatically. Systems should provide audit trails or other methods to track completed disposition actions."

ISO 15489-1, Clause 9.9, "Implementing disposition", provides in part: "The following principles should govern the physical destruction of records –

> 1) Destruction should always be authorized.
> 2) Records pertaining to pending or actual litigation or investigation should not be destroyed.
> 3) Records destruction should be carried out in a way that preserves the confidentiality of any information they contain.
> 4) All copies of records that are authorized for destruction, including security copies, preservation copies and backup copies, should be destroyed."

ISO 15489-1, Clause 9.10, "Documenting records management processes", provides in part: "The documentation should contain details of business activities and the records that result from each business activity, and specify their retention periods and disposition actions clearly and unambiguously. Events that activate or enable disposition actions should be clearly identified. A record of disposition actions, once they have been carried out, should be maintained."

Therefore, ARMA notes that any organization required to establish an Information Security Program pursuant to Regulation S-P, or subject to the FACT Act Disposal Rule,

[16] ISO 15489-1, Clause 3.9 defines "disposition" to mean "range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments". ISO 15489-1, Clause 3.8 defines "destruction" to mean "process of eliminating or deleting records, beyond any possible reconstruction".

should include as an integral part of their Information Security Program a retention and disposition policy for recorded information.

In compliance with ISO 15489-1, Clause 8.3.7, a retention and disposition policy should include the following elements: (1) the identification of the retention period for each covered record, (2) the method of disposal or disposition, and (3) procedures for ensuring compliance.

In compliance with ISO 15489, Clause 9.9, policies regarding the actual disposal of covered records should ensure that: (1) destruction will always be authorized, (2) records pertaining to pending or actual litigation or investigation are not be destroyed, (3) records destruction is carried out in a way that preserves the confidentiality of any information they contain, and (4) all copies of records that are authorized for destruction, including security copies, preservation copies and backup copies, should be destroyed."

Finally, in compliance with ISO 15489, Clause 9.10, proper documentation of any disposal or disposition action should be documented and records of the documentation should be maintained.

IV. ARMA Comments to Proposed Amendments to Regulation S-P

The Commission is proposing amendments to Regulation S–P, which implements certain provisions of GLBA and the FCRA for entities regulated by the Commission. It observes a significant increase in information security breaches involving institutions regulated by the Commission. The Commission further notes that many firms in the securities industry are aware of these problems and have appropriate safeguards in place to address them; however, that some firms do not regularly reevaluate and update their safeguarding programs to deal with these increasingly sophisticated methods of attack.

Subtitle A of Title V of the GLBA requires every financial institution to inform its customers about its privacy policies and practices, and limits the circumstances in which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party without first giving the consumer an opportunity to opt out of the disclosure.

The GLBA specified that standards to be adopted by federal financial regulators were to "insure the security and confidentiality of customer records and information," "protect against any anticipated threats or hazards to the security or integrity" of those records, and protect against unauthorized access to or use of those records or information, which "could result in substantial harm or inconvenience to any customer." In response to these directives, the Commission adopted Regulation S–P in 2000.

Section 30(a) of Regulation S–P (the "Safeguards Rule") currently requires institutions to adopt written policies and procedures for administrative, technical, and physical

safeguards to protect customer records and information and meeting the objectives of GLBA.

Pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), the Commission amended Regulation S–P in 2004 to protect against the improper disposal of consumer report information by adopting Section 30(b) of Regulation S–P (the "Disposal Rule").

With these comments, ARMA attempts to make no observations relative to the conduct of the covered entities specifically or their industry sectors in general. Rather, ARMA accepts the observations of the Commission, and based on these, concludes that Regulation S-P would be strengthened to better reflect the best practices of Records and Information Management, in particular, those practices and procedures that are proven to safeguard records and information from unauthorized use, unintentional disposition or destruction, and to otherwise manage records and information during their entire lifecycle.

The Commission proposes to amend Regulation S–P in four principal ways.

1. To require more specific standards under the safeguards rule, including standards that would apply to data security breach incidents.

2. To amend the scope of the information covered by the safeguards and disposal rules and to broaden the types of institutions and persons covered by the rules.

3. To require institutions subject to the safeguards and disposal rules to maintain written records of their policies and procedures and their compliance with those policies and procedures.

4. To add new exception from Regulation S–P's notice and opt-out requirements to allow investors more easily to follow a representative who moves from one brokerage or advisory firm to another.

ARMA's comments focus primarily on the first and third areas as these provide the opportunity to apply the best practices of Records and Information Management. ARMA further provides general observations about the role of Records and Information Management in safeguarding personally identifiable information, and ARMA re-iterates points it has made relative to the Disposal Rule under the FACT Act.

The proposed changes advocated by ARMA in this submission will be beneficial to entities that operate under the multiple obligations of the different Federal agencies and will enable greater uniformity in practices, to the benefit of the public and the public purposes for which the regulations are being proposed for amendment.

A. Information Security and Security Breach Response Requirements

ARMA agrees with the Commissions statement: "To help prevent and address security breaches at covered institutions, the Commission proposes to require more specific standards for safeguarding personal information, including standards for responding to data security breaches."

As proposed by the Commission, ARMA agrees that the Safeguards Rule should require each covered institution to develop, implement, and maintain a comprehensive "information security program," including written policies and procedures that provide administrative, technical, and physical safeguards for protecting personal information, and for responding to unauthorized access to or use of personal information.

ARMA believes that the Information Security Program as described by the Commission would be most effective by employing the proven elements of a standards-based Records and Information Management Program.

MANAGEMENT INVOLVEMENT: ARMA recommends that the Commission further strengthen the Safeguards Rule by requiring acknowledgement of management's involvement. As cited above in our review of relevant elements of a Records and Information Management Program –

> The importance of executive level support is reflected in ANSI/ARMA standards related to various aspects of records management programs. Section 5.0 of ANSI/ARMA 8-2005, "Retention Management for Records and Information" reinforces the importance of top management support: "The ultimate authority for all decisions relating to retention of records resides with the senior management of the organization." Section 5.2 of the same standard states: "In addition to the information retention and disposition policy statement, senior management should issue specific directives as necessary to ensure support for the information retention and disposition program."[17]

[17] Clause 6.3 of the ISO Standard recognizes that while all employees in an organization have some responsibility for the manner in which organizations keep their records, the level of responsibility and accountability will vary. The standard states: "Records management responsibilities and authorities should be defined and assigned, and promulgated throughout the organization so that, where a specific need to create and capture records is identified, it should be clear who is responsible for taking the necessary action. These responsibilities should be assigned to all employees of the organization, including records managers, allied information professionals, executives, business unit managers, systems administrators and others who create records". Clause 6.3(b) adds more detail specific to executives by stating, "[e]xecutives are responsible for supporting the application of records management policies throughout the organization"

ARMA further agrees that the Information Security Program should be appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of any personal information at issue. This expectation is consistent with the elements of a standards-based Records and Information Management Program.

Also consistent with a standards-based Records and Information Management Program are the particular elements that a program meeting the requirements of Regulation S–P must include:

1. Designate in writing an employee or employees to coordinate the information security program.

A DESIGNATED EMPLOYEE OR EMPLOYEES: ISO 15489, Clause 6.3 "Policies and responsibilities – responsibilities" calls for the assignment of "specific leadership responsibility and accountability" for records management. It further calls for the involvement of "records management professionals" to be involved in "all aspects of records management, including the design, implementation and maintenance of records systems and their operations"

2. Identify in writing reasonably foreseeable security risks that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of personal information or personal information systems.

FORESEEABLE SECURITY RISKS: ISO 27001, Clause 4.2.1 requires an organization to complete a risk assessment that focuses on the assets, threats, vulnerabilities and options for controlling the risks.

3. Design and document in writing and implement information safeguards to control the identified risks.

SAFEGUARDS TO CONTROL RISKS: ISO 27001, Clause 4.2.1 requires an organization, as part of the risk assessment, to identify optional controls and select appropriate controls for the identified risks.

4. Regularly test or otherwise monitor and document in writing the effectiveness of the safeguards' key controls, systems, and procedures, including the effectiveness of access controls on personal information systems, controls to detect, prevent and respond to attacks, or intrusions by unauthorized persons, and employee training and supervision.

TESTING AND AUDITING: As cited above in our review of relevant elements of a Records and Information Management Program –

Section 4.1 of ANSI/ARMA 9-2004 requires that Records and Information Management programs be "regularly reviewed at designated intervals and revised, as needed, to reflect current compliance requirements. Section 7.2 of ANSI/ARMA 8-2004 requires that records management policies authorize individuals within the organization to "monitor equipment, systems, electronic message traffic at any time for security and network maintenance purposes" and that the organization retain authority to "audit networks and systems on a periodic basis to ensure policy compliance".

Section 9.3 of ANSI/ARMA 8-2005 states: "Compliance with the information retention and disposition program is the responsibility of the organization and all employees. Employees should be aware of the program and its requirements – especially the effects of inappropriate or premature disposition of records…Compliance with the information retention and disposition program should be reviewed on a regular basis, determined by organization policy".

Furthermore, Clause 10 of the ISO Standard calls for regular monitoring for compliance and modification to a records management system where policies or outcomes are not being met.

5. Train staff to implement the information security program.

TRAINING AND COMMUNICATION: As cited above in our review of relevant elements of a Records and Information Management Program –

Section 10 of ANSI/ARMA 9-2004 states: "Organizations should provide an ongoing program of user training to facilitate and achieve effective electronic message management. The policy should be communicated to users so that all users are aware of the intent and boundaries of the policy." Section 9.2 of ANSI/ARMA 8-2005 also references the importance of ongoing training in the implementation of an organization's retention and disposition program.

Clause 11 of the ISO Standard addresses the need for training within an organization seeking to comply with the standard. It recognizes that the records management training for employees should be customized to their particular responsibilities and accountability within the program.

ARMA would further recommend that in addition to training, the Commission include an expectation that the Program be properly communicated throughout the enterprise –

Section 4.0 of ANSI/ARMA 9-2004: "The designated records personnel must ensure that the policy is communicated and implemented throughout

the company." The Section also requires that records management policies be published and circulated throughout the organization and that responsibilities for compliance be assigned to every user and each individual with a recordkeeping role, including database administrators and information or network technology support personnel. Section 9.1 of ANSI/ARMA 8-2005 also references the best practice of establishing a manual or processes and procedures relative to records management that is provided to departments and managers throughout an organization.[18]

6. Oversee service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the personal information at issue, and require service providers by contract to implement and maintain appropriate safeguards (and document such oversight in writing).

OVERSIGHT OF SERVICE PROVIDERS: Pursuant to ISO 27001, the need to control risks arising from third parties delivering services is a recognized control objective.[19]

7. Evaluate and adjust their information security programs to reflect the results of the testing and monitoring, relevant technology changes, material changes to operations or business arrangements, and any other circumstances that the institution knows or reasonably believes may have a material impact on the program.

MANAGEMENT OF CHANGE: As indicated earlier, Clause 6.2 of the ISO Standard indicates that "Policies should be regularly reviewed to ensure that they reflect current business needs". Clause 8.4.(h), addressing post-implementation review, indicates that the review of a records system's performance should be "an integral and ongoing process" and that there should be "a regime of continuous monitoring and regular evaluation". Furthermore, pursuant to ISO 27001**,** an organization is required to put into place regular means to monitor and review their information security programs and keep the program aligned to ongoing changes in operations, risks and business arrangements.[20]

---

[18] Section 9.1 of ANSI/ARMA 8-2005 further requires that a letter from the chief executive officer of the organization stating the purpose of the information retention and disposition program and the need for compliance with the policy from all departments and staff. Clause 6.1 of the ISO Standard, addressing policy and responsibilities, states: "An organization seeking to conform to this part of ISO 15489 should establish, document, maintain and promulgate policies, procedures, and practices for records management to ensure that its business need for evidence, accountability and information about its activities is met." Clause 6.2 of the ISO Standard requires that "Organizations should ensure that the policy is communicated and implemented at all levels in the organization. The policy should be adopted and endorsed at the highest decision-making level and promulgated throughout the organization. Responsibilities for compliance should be assigned."

[19] See ISO 27001, Annex A, Section A.10.2 ("Third party service delivery management").
[20] See ISO 27001, Clause 4.2.4.

Under the proposed amendments, institutions subject to the rule would be required to have specific written procedures (itemized below).

These are consistent with ISO 27001; however, ARMA recommends an additional element of these written procedures (highlighted below).

ARMA notes that while these elements anticipate a written report relative to an incident, the language is limited to the steps of remediation taken by the covered entity. It is not clear that records are to be maintained of the incident itself or the investigation. Often those investigations fail to identify the root cause and regulators will need these records available in order to assess the integrity of the investigation process.

1. Assess any incident involving unauthorized access or use, and identify in writing what personal information systems and what types of personal information may have been compromised;

2. Take steps to contain and control the incident to prevent further unauthorized access or use and document all such steps taken in writing;

3. Promptly conduct a reasonable investigation and determine in writing the likelihood that the information has been or will be misused after the institution becomes aware of any unauthorized access to sensitive personal information; and

4. Notify individuals with whom the information is identified as soon as possible (and document the provision of such notification in writing) if the institution determines that misuse of the information has occurred or is reasonably possible.

5. **Establish and maintain records of any incident and the subsequent steps taken in connection with the incident.**

B. Scope of the Safeguards and Disposal Rules

The Commission notes:

> As required under the GLBA, the safeguards rule requires covered institutions to maintain written policies and procedures to protect "customer records and information," which is not defined in the GLBA or in Regulation S–P. The Disposal Rule requires institutions to properly dispose of "consumer report information," a third term, which Regulation S–P defines consistent with the FACT Act provisions.

> Each of these terms includes a different set of information, although the terms include some of the same information. Each term also does *not* include some information that, if obtained by an unauthorized user, could permit access to personal financial information about an institution's customers.

The Commission proposes that "in order to provide better protection against the unauthorized disclosure of this personal financial information, the scope of information protected by both the safeguards rule and the disposal rule should be broader."

ARMA agrees that the Safeguards Rule and Disposal Rule should apply to a consistent set of information. Proper Records and Information Management requires life cycle treatment of any record or information subject to a retention schedule. ARMA also agrees with the Commission that a consistent application of the rules would reduce any burden that may have been created by the application of the safeguards and disposal rules to different information.

ARMA agrees with the Commission's proposal to extend the Safeguards Rule and Disposal Rule to protect "personal information" broadly defined. ARMA supports the Commission's proposal to define that term to encompass any record containing either "nonpublic personal information" or "consumer report information." In addition to nonpublic personal information and consumer report information, "personal information" also would include information identified with any consumer, or with any employee, investor, or security-holder who is a natural person, in paper, electronic or other form, that is handled by the institution or maintained on the institution's behalf.

ARMA would note, however, that a broader category of records of information risks unnecessarily isolating an organization's Records and Information Management Program. While it is appropriate for an organization to identify categories of records of information for special safeguards and management procedures, the applicable regime should not be removed from the broader set of policies and procedures that define the enterprise-wide Records and Information Management Program.

Consistent with ISO 15489-1, Clause 9.3, a broader category of covered states that "Techniques to ensure capture of records may include – a) classification and indexing which allow appropriate linking, grouping, naming, security protection, user permissions and retrieval, disposition, and identifying vital records …"[21]

C. Records of Compliance

The Commission proposes to amend Regulation S–P to require covered institutions to make and preserve written records of their safeguards and disposal policies and procedures. The Commission also proposes to require that institutions document that they

[21] For guidance on classification systems, see ISO 15489-1, Clause 9.5.

have complied with the elements required to develop, maintain and implement these policies and procedures for protecting and disposing of personal information, including procedures relating to incidents of unauthorized access to or misuse of personal information.

Compliance documentation is a core component of any Records and Information Management Program.[22]

ARMA further agrees that these records would help institutions assess their policies and procedures internally, and help examiners to monitor compliance with the requirements of the amended rules.

It is appropriate that the periods of time for which the records would have to be preserved would vary by institution, because the requirements would be consistent with existing recordkeeping rules, beginning with when the records were made, and, for records of written policies and procedures, after any change in the policies or procedures they document.

D. Exceptions for Limited Information Disclosure When Personnel Leave Their Firms

The Commission proposes to amend Regulation S–P to add a new exception from the notice and opt-out requirements to permit limited disclosures of investor information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser moves from one brokerage or advisory firm to another. The Commission explains that the proposed exception is intended to allow firms with departing representatives to share limited customer information with the representatives' new firms that could be used to contact clients and offer them a choice about whether to follow a representative to the new firm.

V. Cost-Benefit Analysis of a Records and Information Management Program

The Commission seeks comments on the value of benefits derived from the proposed amendments to Regulation S-P.

Records and Information Management can and does reduce the costs of compliance. The very basis of Records and Information Management is compliance based on a set of enterprise-wide processes and procedures to enable every day business practices to comply with business-specific as well as statutory and regulatory requirements.

[22] See ISO 27001, Clause 4.3.3, describing the obligation for organizations to create and maintain records regarding their information security management program and activities. See also ISO 15489-1, Clause 9.10 "Documenting Records Management Processes".

> *Records contain information that is a valuable resource and an important business asset. 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.*[23]

The proposed amendments would modify Regulation S–P's current safeguards and disposal rules to:

(i) Require more specific standards under the safeguards rule, including standards that would apply to data security breach incidents;

(ii) Broaden the scope of information and the types of institutions and persons covered by the rules; and

(iii) Require covered institutions to maintain written records of their policies and procedures and their compliance with those policies and procedures.

The Commission has expressed concern that some institutions do not regularly reevaluate and update their safeguarding programs. Requiring covered institutions to designate in writing an employee or employees to coordinate their information security programs should foster clearer delegations of authority and responsibility, making it more likely that an institution's programs are regularly reevaluated and updated. Having an information security program coordinator also could contribute to an institution's ability to meet its affirmative and continuing obligation under the GLBA to safeguard customer information.136

If, for example, elements of a covered institution's information security program were not maintained on a consolidated basis, but were dispersed throughout an institution, we believe having a responsible program coordinator or coordinators should facilitate the institution's awareness of these elements, as well as enable it to better manage and control risks and conduct ongoing evaluations.

In general, ARMA agrees that "the proposed framework for the initial and ongoing oversight of institutions' information security programs—in the form of formal risk assessments, periodic testing or monitoring of key controls, systems, and procedures, staff training, and relevant evaluations and adjustments—would help to ensure that information security programs are appropriately updated along with relevant changes in

[23] See ISO 15489-1, Clause 4 "Benefits of records management".

technology, new business arrangements, changes in the threat environment, and other circumstances."

Finally, the proposed amendment that would require covered institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards and would require service providers by contract to implement and maintain appropriate safeguards should help to ensure that sensitive personal information is protected when it leaves the institution's custody, while still permitting institutions the flexibility to select appropriate service providers.

VI. Specific Recommendations to the Proposed New Text of the Safeguards Rule and the Disposal Rule

ARMA recommends the following additional text to the proposed Safeguards and Disposal Rules (**recommended text is underlined and in bold text**):

§ 248.30 Information security programs for personal information; records of compliance.

(a) *Information security programs.—*

(1) *General requirements.* Every broker or dealer other than a notice-registered broker or dealer, every investment company, and every investment adviser or transfer agent registered with the Commission, must develop, implement, and maintain a comprehensive information security program. Your program must include written policies and procedures that provide administrative, technical, and physical safeguards for protecting personal information, and for responding to unauthorized access to or use of personal information. **Your program must be approved by senior management, communicated across your enterprise, and be supported with adequate training and auditing processes to ensure compliance.** Your program also must be appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any personal information at issue. **In developing and managing your program, you should take account of standards-based Records and Information Management practices and procedures, and your information security program should be integrated with the enterprise-wide programs and procedures for records and information management otherwise required to be maintained.**

(2) *Objectives*. Your information security program must be reasonably designed to:

(i) Ensure the security and confidentiality of personal information;

(ii) Protect against any anticipated threats or hazards to the security or integrity of personal information; and

(iii) Protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience to any consumer, employee, investor or security-holder who is a natural person.

(3) *Safeguards*. In order to develop, implement, and maintain your information security program, you must:

(i) Designate in writing an employee or employees to **manage and** coordinate your information security program;

(ii) Identify in writing reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information and personal information systems that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information or systems;

(iii) Design and implement safeguards to control the risks you identify, and maintain a written record of your design;

(iv) Regularly test or otherwise monitor, and maintain a written record of the effectiveness of the safeguards' key controls, systems, and procedures, including the effectiveness of:

(A) Access controls on personal information systems;

(B) Controls to detect, prevent and respond to incidents of unauthorized access to or use of personal information; and

(C) Employee training and supervision relating to your information security program.

(v) Train staff to implement your information security program;

(vi) Oversee service providers, and document in writing that in your oversight you are:

(A) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the personal information at issue; and

(B) Requiring your service providers by contract to implement and maintain appropriate safeguards; and

(vii) Evaluate and adjust your information security program accordingly in light of:

(A) The results of the testing and monitoring required by paragraph (a)(3)(iv) of this section;

(B) Relevant changes in technology;

(C) Any material changes to your operations or business arrangements; and

(D) Any other circumstances that you know or reasonably believe may have a material impact on your information security program.

(4) *Procedures for responding to unauthorized access or use*. At a minimum, your information security program must include written procedures to:

(i) Assess the nature and scope of any incident involving unauthorized access to or use of personal information, and maintain a written record of the personal information systems and types of personal information that may have been accessed or misused;

(ii) Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of personal information and maintain a written record of the steps you take;

(iii) After becoming aware of an incident of unauthorized access to sensitive personal information, promptly conduct a reasonable investigation, determine the likelihood that the information has been or will be misused, and maintain a written record of your determination;

(iv) If you determine that misuse of the information has occurred or is reasonably possible, notify each individual with whom the information is identified as soon as possible in accordance with paragraph (a)(5) of this section and maintain a written record that you provided notification; provided however that if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and requests in writing that you delay notification, you may delay notification until it no longer interferes with the criminal investigation; and

(v) If you are a broker or dealer other than a notice-registered broker or dealer, provide written notice on Form SP–30 to your designated examining authority (*see* 17 CFR 240.17d–1), and, if you are an investment company or an investment adviser or transfer agent registered with the Commission, provide written notice on Form SP–30 to the principal office of the Commission, as soon as possible after you

become aware of any incident of unauthorized access to or use of personal information in which:

(A) There is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience; or

(B) An unauthorized person has intentionally obtained access to or used sensitive personal information.

(5) *Notifying individuals of unauthorized access or use*. If you determine that an unauthorized person has obtained access to or used sensitive personal information, and you determine that misuse of the information has occurred or is reasonably possible, you must notify each individual with whom the information is identified in a clear and conspicuous manner and by a means designed to ensure that the individual can reasonably be expected to receive it.

The notice must:

(i) Describe in general terms the incident and the type of sensitive personal information that was the subject of unauthorized access or use;

(ii) Describe what you have done to protect the individual's information from further unauthorized access or use;

(iii) Include a toll-free telephone number to call, or if you do not have any toll-free number, include a telephone number to call and the address and the name of a specific office to write for further information and assistance;

(iv) If the individual has an account with you, recommend that the individual review account statements and immediately report any suspicious activity to you; and

(v) Include information about the availability of online guidance from the FTC regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and the FTC's Web site address and toll-free telephone number that individuals may use to obtain the identity theft guidance and report suspected incidents of identity theft.

(b) *Disposal of personal information*.—(1) *Standard*. Every broker or dealer other than a notice-registered broker or dealer, every investment company, every investment adviser or transfer agent registered with the Commission, and every natural person who is an associated person of a broker or dealer, a supervised person of an investment adviser registered with the Commission, or an associated person of a transfer agent registered with the Commission, that maintains or otherwise possesses personal information for a

business purpose must properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(2) *Written policies, procedures and records*. Every broker or dealer, other than a notice-registered broker or dealer, every investment company, and every investment adviser and transfer agent registered with the Commission must:

(i) Adopt written policies and procedures that address the proper disposal of personal information according to the requirements of paragraph (b)(1) of this section; and

(ii) Document in writing its proper disposal of personal information in compliance with paragraph (b)(1) of this section.

Your program must be approved by senior management, communicated across your enterprise, and be supported with adequate training and auditing processes to ensure compliance. In developing and managing your program, you should take account of standards-based Records and Information Management practices and procedures, and your information security program should be integrated with the enterprise-wide programs and procedures for records and information management otherwise required to be maintained.

(3) *Relation to other laws*. Nothing in this paragraph (b) shall be construed:

(i) To require any broker, dealer, investment company, investment adviser, transfer agent, associated person of a broker or dealer, supervised person of an investment adviser, or associated person of a transfer agent, to maintain or destroy any record pertaining to an individual that is not imposed under other law; or

(ii) To alter or affect any requirement imposed under any other provision of law to maintain or destroy records.

(c) *Recordkeeping*. (1) Every broker or dealer other than a notice-registered broker or dealer, every investment company, and every investment adviser or transfer agent registered with the Commission, must make and maintain the records and written policies and procedures required under paragraphs (a) and (b)(2) of this section. Every broker or dealer other than a notice-registered broker or dealer, and every investment adviser registered with the Commission seeking to rely on the exception in § 248.15(a)(8) must make and maintain the records required by § 248.15(a)(8)(iii).

(2) Starting from when the record was made, or from when the written policy or procedure was last modified, the records and written policies and procedures required

under paragraphs (a) and (b)(2) of this section, and the records made pursuant to § 248.15(a)(8)(iii), must be preserved in accordance with:

(i) 17 CFR 240.17a–4(b) by a broker or dealer other than a notice-registered broker or dealer;

(ii) 240.17Ad–7(b) by a transfer agent registered with the Commission;

(iii) 270.31a–2(a)(4)–(6) by an investment company; and

(iv) 275.204–2(e)(1) by an investment adviser registered with the Commission.

(d) *Definitions.* As used in this § 248.30, unless the context otherwise requires:

(1) *Associated person of a broker or dealer* has the same meaning as in section 3(a)(18) of the Securities Exchange Act of 1934 (15 U.S.C.78c(a)(18)).

(2) *Associated person of a transfer agent* has the same meaning as in section 3(a)(49) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(49)).

(3) *Consumer report* has the same meaning as in section 603(d) of the Fair Credit Reporting Act (15 U.S.C.1681a(d)).

(4) *Consumer report information* means any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report. Consumer report information also means a compilation of such records. Consumer report information does not include information that does not identify individuals, such as aggregate information or blind data.

(5) *Disposal* means:

(i) The discarding or abandonment of personal information; or

(ii) The sale, donation, or transfer of any medium, including computer equipment, on which personal information is stored.

(6) *Information security program* means the administrative, technical, or physical safeguards you use to **manage the life cycle of a record of personal information, including** access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

(7) *Notice-registered broker or dealer* means a broker or dealer registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 .S.C. 78o(b)(11)).

(8) *Personal information* means any record containing consumer report information, or nonpublic personal information as defined in § 248.3(t), that is identified with any consumer, or with any employee, investor, or security-holder who is a natural person, whether in paper, electronic, or other form, that is handled or maintained by you or on your behalf.

(9) *Personal information system* means any method used to access, collect, store, use, transmit, protect, or dispose of personal information.

NEW DEFINITION: (10) *Records and Information Management Program* means a defined process for achieving 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

(10) *Sensitive personal information* means personal information, or any combination of components of personal information, that would allow an unauthorized person to use, log into, or access an individual's account, or to establish a new account using the individual's identifying information, including the individual's:

(i) Social Security number; or

(ii) Name, telephone number, street address, e-mail address, or online user name, in combination with the individual's account number, credit or debit card number, driver's license number, credit card expiration date or security code, mother's maiden name, password, personal identification number, biometric record, or other authenticating information.

(11) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a broker, dealer, investment company, or investment adviser or transfer agent registered with the Commission.

(12) (i) *Substantial harm or inconvenience* means personal injury, or more than trivial financial loss, expenditure of effort or loss of time, including theft, fraud, harassment, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the unauthorized use of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise use the individual's account.

(ii) Substantial harm or inconvenience does not include unintentional access to personal information by an unauthorized person that results only in trivial financial

loss, expenditure of effort or loss of time, such as if use of the information results only in your deciding to change the individual's account number or password.

(13) *Supervised person of an investment adviser* has the same meaning as in section 202(a)(25) of the Investment Advisers Act of 1940 (15 U.S.C. 80b–2(a)(25)).

(14) *Transfer agent* has the same meaning as in section 3(a)(25) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(25)).