Before the
Securities and Exchange Commission

In the Matter of
Disposal of Consumer Report Information
File Number S7-33-04

COMMENTS OF

ARMA INTERNATIONAL

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 professional. The 10,000 members of ARMA include records and information managers, imaging specialists, archivists, librarians, and educators in both the public and private sectors.

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 – a program that best practices demonstrate should be in writing, approved by senior management, supported by appropriate budget and training, given appropriate attention and seriousness through risk assessments and audits, and acknowledged as a firm-wide policy. An organization's disposal of records of information, such as "consumer information" in the instance of the proposed amendments to Commission's Safeguard Rule, 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.

As a recognized standard developer for the American National Standards Institute (ANSI), ARMA has submitted for public comment "Managing Recorded Information Assets and Resources: Retention and Disposition Program" (hereafter "the Draft Standard"). These are submitted as a part of ARMA's comments by reference to the ARMA web page. See http://www.arma.org/standards/documents/RetentionDispositionGuidelinePublicReview0504.pdf.

While the Draft Standard is still open for public comment and has not completed the formal ANSI standards development process, it represents long recognized best practices for the retention and disposition of information in the custody of organizations in both the

public and private sectors. ARMA believes it would find application for entities covered by the Commission's Safeguard Rule and the proposed disposal requirement.

The Draft Standard in part updates an earlier ARMA publication, entitled "Developing and Operating a Records Retention Program – A Guide" (hereafter "ARMA 1986 Guide"), developed under ARMA's standards making process. For excerpts of this document, see "Guidelines for Retention by Industry Program (GRIP)" at www.arma.org/membership/isg/grip. For example, the Draft Standard incorporates electronic records, and it acknowledges those best practices that have since become supported by legislative and judicial action.

An additional source of the best practices of information management may be found in the International Organization for Standardization (ISO) International Standard, "Information and documentation – Records management – Part 1: General" (ISO 15489-1:2001) (hereafter "ISO 15489-1"). ARMA is 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.[1]

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

During consideration of the Fair and Accurate Credit Transactions (FACT) Act (Pub. L. 108-159) 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."

[1] 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.

Long recognized in the field of 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 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 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." See ARMA 1986 Guide. 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." See Draft Standard, Introduction.

Of the core elements of an information retention and disposition program that ARMA recommends to the Commission for consideration 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.

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. It also supports the ability of the Commission during enforcement actions or investigations.

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's comments are therefore informed by the importance of a formal, written information retention and disposition program. 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. ARMA notes that the Commission's Safeguard Rule provides the basis for ensuring that covered entities have in place a retention and disposition program that includes the elements recognized by the field of information management.

ARMA's comments are also 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.[2] 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.

[2] 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". Similarly, Draft Standard, Section 3, "Definitions," defines "disposition" to mean "a range of processes associated with implementing records retention, destruction, or transfer decisions that are documented in the records retention and disposition schedule or other authorities. Draft Standard, Section 3 defines "destruction" to mean "the process of eliminating or deleting records beyond any possible reconstruction."

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 recommends that the Commission ensure that covered entities include as a part of their information security programs a retention and disposition policy for recorded information covered by the Safeguard Rule.

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 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.

III. ARMA Comments to the Proposed Amendments to the Commission's Safeguard Rule, Section 30 of Regulation S-P.

The proposed amendments to the Safeguard Rule would require covered entities to take "reasonable measures to protect against unauthorized access to or use of [consumer report information] in connection with its disposal." The proposed amendments define "consumer report information" and "disposal". The proposed amendments would require a covered entity to adopt information safeguard policies and procedures in writing.

A. In General.

ARMA agrees that the new proposed disposal requirements be made a part of the Commission's Safeguard Rule. As discussed, the retention and disposition policies and procedures must be a part of a covered entity's information security program. ARMA also strongly agrees that information safeguard policies and procedures must be in writing. ARMA further strongly urges the Commission to ensure that senior management is fully aware and supportive of these policies and procedures, that risk assessments are required for any disposal policies and procedures, that training be documented and budgeted for a covered entity's employees with information management responsibilities or custodial responsibility of consumer report information, and that service provider arrangements address any disposal requirements.

B. Definitions.

1. Definition of "Consumer Report" and "Consumer Report Information".

The Commission proposes a definition of "consumer report" to have the same meaning as in section 603(d) of the FCRA. The Commission proposes a definition of "consumer report information" to mean "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report." The proposed disposal requirement would apply to both consumer reports and consumer report information.

The Commission intends that this provide a broad definition of the information covered by the proposed disposal requirement.

ARMA believes that any record on a consumer, maintained for a business purpose, containing information that is personally identifiable in nature, should be subject to the disposal requirement. This should address the Commission's intent that the proposed disposal requirement apply only to information that "identifies particular individuals".

ARMA also supports the proposed text that includes not only "consumer report information" but also "any compilation of consumer report information."

However, ARMA notes that recognized best practices regarding the disposal of any record created by a business entity be included in the entity's document retention and disposition policies and procedures. ARMA urges the Commission to be mindful that a comprehensive approach to an entity's retention and disposition policies and procedures will most likely support the stewardship of consumer reports and consumer report information anticipated in this proposed change to the Safeguard Rule.

ARMA's Draft Standard includes the following definition of "record":

> "Recorded information, regardless of medium or characteristics, made or received by an organization that is evidence of its operations, and has value requiring its retention for a specific period of time. Recorded

> information in any format that is created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. Records have these characteristics: authenticity (it is what it says it is), reliability (it can be trusted as a full and accurate representation of the transactions or facts), integrity (it is complete and unaltered), and usability (it can be located, retrieved, presented, and interpreted)."

ISO 15489-1 defines "records" as –

> "Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business."

To provide more comprehensive and less ambiguous application of the proposed disposal requirements, ARMA recommends the following addition to the definition of covered information:

"any record, records system, document, file, or other media containing data, including any recorded information, about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the covered entity for a business purpose, including "a compilation of such records".

2. Definition of "Disposal".

The Commission proposes a definition of "disposal" to mean "the discarding or abandonment of consumer report information," and "the sale, donation, or transfer of any medium, including computer equipment, on which consumer report information is stored."

As discussed below in conjunction with the meaning of "proper disposal," ARMA strongly urges the Commission to revisit this definition. Disposal should be acknowledged as a part of the overall retention and disposition of information in the custody of a covered entity, requiring specific actions on the part of the custodian of the covered information. Disposal, as it relates to the life cycle of information, is not so much about the physical disposal of equipment or the intent to be rid of records of information; rather, it is about the proper management of information based on its life cycle within an organization.

C. Inclusion of Disposal Requirement in Retention and Disposition Policies and Procedures.

ARMA urges the Commission to make clear that the proposed disposal requirement be made a part of the policies and procedures required under its Safeguard Rule, now proposed to be in writing.

Recognized best practices of information management require a formally adopted, written program of policies and procedures. These policies and procedures, when acknowledged as part of the business practices of an organization, will better ensure compliance, will provide a source of training for employees and personnel responsible for the management of consumer information, and will enable more meaningful enforcement for the Commission if and when a covered entity is suspected of or charged with impermissible practices.

A properly implemented retention and disposition program, with appropriate control mechanisms and assignment of responsibility, will also ensure senior management support and responsibility regarding the stewardship of the information covered by the Safeguard Rule. The ARMA 1986 Guide provides that senior management support "should take the form of a policy statement establishing the records retention and disposition program as a part of an overall records management program, directives to organizations managers and staff to cooperate with the program, and on-going funding and support for the program."

Inclusion of new disposal requirements as a part of a covered entity's information security program will also ensure appropriate staff training and attention to any specific policies and procedures established for the disposal of covered consumer and customer information. Draft Standard, Section 9.2 provides:

> "Ongoing training in the use of and compliance with the information retention and disposition [program] is an important part of the implementation … and should be provided by the records manager and other members of the organization. During these sessions, problems related to the program can be discussed and rectified, and, if necessary, changes made to the procedures or retention schedule. Training will also be necessary on an individualized basis for new department information coordinators and for departments experiencing specific recorded information problems."

D. New Provision to Require the Proper Disposal of Covered Information.

The Commission proposes to require each covered entity to "properly dispose of [consumer report information] by taking reasonable measures to protect against unauthorized access to or use or the information in connection with its disposal."

1. Covered Entities.

The proposed application of the disposal requirement is limited to an entity that "maintains or otherwise possesses consumer report information or any compilation of consumer report information for a business purpose."

Information is an essential asset for businesses that will possess, maintain, and process consumer information. Any information that is essential to the business purpose of an organization should be subject to the Safeguard Rule. This should not impose a burden on covered entities; instead, information retention and disposition programs create efficiencies in the management of any such information and other organizational benefits.

Draft Standard, Section 4.2, "Benefits of an Information Retention and Disposition Program" notes improved operational efficiencies, consistency in records disposition, compliance with legal and regulatory retention requirements, protection during litigation or government investigation, reduced space requirements, and cost containment.

ISO 15489-1, Clause 7.1 provides: "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. To do this, organizations should institute and carry out a comprehensive records management programme…"

ARMA strongly urges the Commission to ensure that the term "for a business purpose" retain a very broad interpretation. ARMA believes that any information that is personal and identifiable in the custody of a covered entity will be retained and maintained as a record for a business purpose.

2. Guidelines for "Proper Disposal".

The proposed text regarding "proper disposal" does not include a description of or provide guidance on proper methods of disposal. In its proposed definition of "disposal," the Commission offers a limited set of actions that may or may not be taken by a covered entity. The proposed text does not provide a standard against which a covered entity can be held accountable to or measure its success in maintaining and implementing its safeguards.

Furthermore, the Commission provides little if any guidance as to the meaning of "proper," other than its qualification of "reasonable measures". Taken together, ARMA believes that the text is ambiguous. ARMA strongly recommends that the Commission provide clarification or point to best practices developed in the field of information management.

ARMA recommends that the Commission include a specific definition for the term "proper disposal" or otherwise provide clear guidance and articulation of the elements of "proper disposal".

ARMA's Draft Standard and ISO 15489-1 both define "destruction" as –

> "Process of eliminating or deleting records, beyond any possible reconstruction."

ARMA notes that this definition refers to "disposal" as a "process". Disposal of recorded information is in fact a series of actions to be taken consistent with an organization's retention and disposition policies and procedures.

Draft Standard, Section 10.4, "Destruction of Recorded Information", provides the following specific guidance for proper disposal –

> "The information retention and disposition program shall require documentation that the recorded information was physically destroyed (paper/microform-based information) or was deleted and the media was overwritten (disk/diskette/tape/CD-RW-based electronic recorded information). Deleting indices or pointers to electronic data is not sufficient without deleting the recorded information itself. Each user must use the approved retention schedules to ensure that all electronic recorded information on personal computers, diskettes, and other electronic storage media under the user's control is deleted at the end of the approved retention period. Likewise, the information technology department must include approved retention periods into data set management procedures to ensure that information recorded onto magnetic tapes is deleted or overwritten, or the tapes are physically destroyed at the expiration of the retention period."

> "When recorded information is destroyed or deleted, the date and the signature of the records manager or his/her delegate should be placed on the Destruction Authorization form. If someone other than the records manager witnessed the actual destruction, that individual should sign the destruction form. Destruction information should be noted in the records management system to provide an audit trail. A record of the destruction should be kept to show systematic destruction and to explain the destruction procedures if this information is requested in litigation or

government investigation. A retention period for destruction authorizations and related records of destruction shall be established by the records manager and approved by the Records Information Retention Committee."

"Recorded information shall be destroyed in a controlled, supervised environment. Confidential or proprietary information, requiring supervised or specialized forms of destruction, such as shredding or pulping, shall be destroyed under the supervision of the records manager or designated representative. The records manager shall sign a statement related to the form of destruction and attach documentation for destruction services received from outside sources verifying that the destruction has, in fact, taken place."

"Recorded information that is not confidential or proprietary and is paper-based or microform based may be recycled. Electronic information recorded onto a hard disk, diskette, or rewriteable CD shall be deleted and all unused space on the disk/diskette shall be overwritten, using a utility program to minimize the potential for recovery of the recorded information. Electronic information recorded onto a magnetic tape shall be deleted and the tape overwritten or physically destroyed to minimize the potential for recovery of the recorded information. Nonrewriteable CDs shall be physically destroyed to eliminate the potential for recovery of the recorded information."

ARMA recommends that the Commission replace its proposed text for the descriptor of "proper disposal" to better and more closely reflect the definition recognized by the best practices of information management and to provide a clear standard against which covered entities may measure their own practices and against which covered entities may be held accountable.

3. Guidelines for "Reasonable Measures".

The Commission notes that "there are few foolproof methods of record destruction," and therefore it proposes a standard that will not require "perfect destruction of consumer report information in every instance." Instead, the Commission proposes an ambiguous guidance of requiring that "reasonable measures" be taken to ensure against unauthorized access to or use of the information in connection with its disposal.

The Commission notes that the term "reasonable measures" may include the sensitivity of the information, the size of the entity and the complexity of the operations. The Commission also notes that reasonable measures "may require elements such as the establishment of policies and procedures governing disposal, as well as employee training."

ARMA agrees with the Commission's observations; however, believes that these and other minimum required elements of any entity's information retention and disposition program should be identified in the text of the Safeguard Rule. ARMA notes that unambiguous elements of a retention and disposition program not only create a regime of practice in an organization that guards against unintended and harmful disposition of information, but also creates protection for the organization in instances of regulatory and legal action.

ARMA strongly urges the Commission to further address this proposed text. The best practices of information management identify core elements that should be a part of any retention and disposition policy. At a minimum, these include risk assessment, auditing and testing, training, involvement of senior management, and documentation.

ARMA agrees that a regime of retention and disposition should be flexible to allow covered entities to make decisions appropriate to their particular circumstances and should minimize the disruption of existing practices to the extent that they already provide appropriate protections. ARMA notes that the very contribution of a written, formally adopted, retention and disposition program is to provide flexibility and to capture known best practices unique to an entity or an industry sector. However, without defining these as a policy to be followed by employees and business affiliates of a covered entity, any and all safeguards, whether they be safeguards against unauthorized access during the useful life of a record or during the disposal process, subjects the entire regime to ad hoc decision making and threatens internal compliance. It also makes oversight and enforcement difficult if not impossible.

ARMA strongly urges the Commission to ensure that the disposal of covered information be properly documented by covered entities. Documentation of the disposition and disposal of information is an essential and recognized element of information management. It provides evidence of compliance with an organization's document retention policy – as well as compliance with regulatory and statutory regimes. Such documentation, in compliance with an organization's retention and disposition policies and procedures, provides a threshold level of evidence for oversight and enforcement of the proposed rule. Documentation also instills an important discipline in the actions taken to dispose of recorded information.

Draft Standard, Section 2.6.4.4, "Destruction Documentation" provides:

> "When records are destroyed, the date and the records manager's signature should be placed on the destruction authorization form. Destruction information should also be noted in the records center index and appropriate records transfer list. The record of destruction should be kept long enough to show systematic destruction and to explain the destruction procedures if this information is requested in litigation or government investigation."

Draft Standard, Section 2.6.4.5, "Confidential information" provides:

> "Confidential or proprietary information, requiring supervised or specialized forms of destruction (such as shredding or pulping), should be destroyed under the supervision of the records manager or designated representative. The records manager should also sign a statement related to the form of destruction and attach documentation for destruction services received from outside sources."

Draft Standard, Section 4.2, "Benefits of an Information Retention and Disposition Program" notes that "Compliance with the retention and disposition program allows the organization to demonstrate that it manages its recorded information in the regular course of business and in accordance with a sound business policy and applicable laws and regulations. Demonstrating organizational compliance with program policies and procedures is critical for establishing the organization's credibility regarding litigation issues and the appropriate destruction of records and information is important."

ARMA recommends that "proper disposal" be defined to mean at a minimum "the process of eliminating or deleting records beyond any possible reconstruction, which shall be documented as a part of the covered entity's information security program".

IV. <u>Summary of ARMA Recommendations</u>.

ARMA recommends that the following be adopted as part of the proposed amendments to the Guidelines –

1. The policies and procedures required by the Safeguard Rule should include specific retention and disposition policies and procedures, including those addressing the new disposal requirements.

2. The new requirement that the policies and procedures anticipated under the Safeguard Rule should not only be in writing, but should also be formally adopted by senior management and supported by risk assessments, testing and training.

3. The definitions for "customer report information" should be expanded to include "any record, records system, document, file, or other media containing data, including any recorded information, about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of a covered entity for a business purpose, including a compilation of such records".

4. The term "proper disposal" should be defined to mean at a minimum "the process of eliminating or deleting records, beyond any possible reconstruction, which shall be documented as a part of the covered entity's information security program".

5. At a minimum, the required disposal of consumer report information should include a requirement that the disposal event be documented.

Respectfully submitted,

ARMA International

By:

David McDermott, CRM
President
ARMA International
13725 West 109th Street, Suite 101
Lenexa, KS 66215
(800) 422-2762

Frank Moore
Government Relations Counsel
SmithBucklin Government Relations
2025 M Street, NW, Suite 800
Washington, DC 20036
(202) 367-1254

October 20, 2004
Submitted Electronically