Before the
Board of Governors of the Federal Reserve System
And
Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation
Office of Thrift Supervision

In the Matter of
The FACT Act Disposal Rule, Docket No. R-1199

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 profession. The 10,000 members of ARMA include records and information managers, imaging specialists, archivists, librarians, and educators.

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.

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, and would find application for financial institutions.

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 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.[1]

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

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." [underlining 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 information management, the "protocols" referred to by Senator Nelson that outline the proper way to dispose of records and information are

[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.

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 Agencies 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.

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'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'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.
> 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."

[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."

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 Agencies ensure that covered institutions include as a part of their information security programs a retention and disposition policy for recorded information covered by the Guidelines.

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.

III. ARMA Comments to the Proposed Amendments to the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

The proposed amendments to the Guidelines would require financial institutions to implement controls designed to ensure the proper disposal of "consumer information" within the meaning of section 216 of the FACT Act. The proposed amendments would require a financial institution to dispose of "consumer information" derived from a consumer report in a manner consistent with the existing requirements that apply to the disposal of "customer information".

A. Scope.

ARMA agrees that the Guidelines must clearly indicate coverage of any new requirements regarding the disposal of consumer information. Inclusion of the proposed text in the section defining the scope of the Guidelines is an appropriate means of incorporating the disposal requirements in the current framework of the Guidelines. As discussed in more detail below, the retention and disposition policies and procedures must be a part of the institution's information security program, subject to all of the

requirements of the Guidelines. This should ensure that senior management is fully aware and supportive of its provisions, that the required risk assessment are applicable to any disposal policies and procedures, that training includes any appropriate details regarding disposal of consumer information, and that service provider arrangements address any disposal requirements.

B. Definitions.

1. Definition of "Consumer Information".

The Agencies propose a definition of "consumer 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 and that is maintained or otherwise possessed by or on behalf of the [institution] for a business purpose", including "a compilation of such records".

ARMA notes that the current Guidelines include the definition of "customer information" to mean "any record containing nonpublic personal information … about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the [institution]".

Both the definition for the term "consumer information" and the term "customer information" use the term "record".

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."

The Agencies should expand the definition of both "consumer information" and "customer information" to include not only the term "record", which as defined above

could be read to be limited to only certain consumer information and customer information, but to also include additional terms that will capture all possible recorded data that may be created containing consumer or customer information.

Specifically, ARMA recommends the following definition for "consumer 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 [institution] for a business purpose", including "a compilation of such records".

2. Identification of non-covered consumer or customer information.

ARMA urges the Agencies to ensure that the combined definitions of "consumer information" and "customer information" clearly include any record, records system, or recorded information associated with any consumer data intended to be covered by the Guidelines, whether or not derived from a consumer report. ARMA notes the Agencies' acknowledgement that the scope of information covered by the terms "consumer information" and "customer information" as defined by the Guidelines will sometimes, but not always, overlap. ARMA believes that this reveals a possible source of confusion that may undermine the best developed and implemented information security program. Information retention and disposition policies must clearly identify covered information. To the extent that the definitions for "consumer information" and "customer information" may create confusion, and data on consumers or customers therefore rely on subjective decision making regarding applicability of any Guideline requirements, ARMA recommends that the Guidelines, and the written information security programs developed by institutions, clearly state what information is covered, identifying all possible points of confusion as part of the program's risk assessment and risk controls.

ARMA also observes, that to the extend that both consumer information and customer information are covered by the Guidelines, records derived from any information that falls within the definition of either term should be subject to the same safeguards and disposal requirements.

ARMA believes that a consistent application of retention and disposal requirements to records containing nonpublic personal information and personally identifiable information within the meaning of both definitions will ensure greater compliance with the Guidelines and greater safeguards for the covered information. This is consistent with the Agencies' intention that consumer information be disposed of in a manner consistent with the disposition of customer information.

3. Business Purpose.

The proposed definition of "consumer information" also includes a qualification that covered "consumer information" be "derived from a consumer report and that is maintained or otherwise possessed 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 amended Guidelines. This should not impose a burden on institutions; 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…"

C. New Objective for an Information Security Program.

The proposed amendments would require a financial institution to design its information security program to "[e]nsure the proper disposal of consumer information in a manner consistent with the disposal of customer information".

1. New Objective.

ARMA strongly supports the inclusion of a specific new objective within the scope of an institution's information security program for reasons relating to recognized best practices of retention and disposition programs. ARMA urges the Agencies to eliminate any doubt that the "proper disposal" of and the "appropriate disposal procedures" for covered consumer and customer information must be a part of the institution's written information security program. This is particularly important with respect to the development and implementation of the information security program, which under Section III of the Guidelines require senior management involvement, risk assessments and management and control of identified risks.

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 institution, 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 Agencies if and when an institution 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 Guidelines. 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 an institution'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."

2. Applicability of Guidelines.

ARMA concurs that this new objective will ensure consistent application of the Guidelines regarding the disposal of covered information. Such requirements must be applicable to service providers, data processors, and other entities and organizations in the chain of custody of "consumer information" and "customer information", and ARMA urges the Agencies to ensure that all third party relationships with an institution include a formal articulation of the institution's obligations under the Guidelines. An information security program must follow the life cycle and custody of all covered information in order to be effective.

D. New Provision to Implement Measures to Properly Dispose of Consumer Information.

The proposed amendments would require an institution to develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of consumer information.

1. Definition for "Proper Disposal".

The proposed amendments do not include a description of the proper methods of disposal. The Agencies indicate their belief that it is not necessary to propose a "prescriptive" rule describing methods of disposal, and ARMA does not suggest that specific methods of disposal be imposed by the Guidelines. However, the Agencies note that institutions will be expected "to have appropriate disposal procedures for records maintained in paper-based or electronic forms". The Agencies further note that "an institution's information security program should ensure that paper records containing either customer or consumer information should be rendered unreadable as indicated by the institution's risk assessment, such as by shredding or other means". The Agencies also note the unique issues involving the disposal of "computer-based records". Yet these are not included in the text of the proposed amendments.

ARMA recommends that the Agencies 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."

2. Documentation of Disposition and Disposal.

ARMA strongly urges the Agencies to ensure that the disposal of covered information be properly documented by the institutions. 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 institution's information security program".

E. Proposed Amendments to the Agencies' FCRA Regulations.

The Agencies propose to amend their respective FCRA regulations by adding a new provision setting forth the duties of users of consumer reports regarding identity theft. The proposed amendments would require a financial institution to properly dispose of consumer information in accordance with the standards set forth in the Guidelines.

ARMA strongly supports these amendments to existing FRCA regulations. Because information management programs must reflect any and all regulatory requirements regarding the retention and disposition of recorded information, all regulatory regimes that cover common data and recorded information should point to and acknowledge consistent requirements for the development and implementation of information management programs.

IV. Summary of ARMA Recommendations.

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

1. The information security programs of covered institutions should include specific retention and disposition policies and procedures.

2. The definitions for "consumer information" and "customer information" should be expanded to include "any record, records system, document, file, or other media containing data, including any recorded information, about an individual".

3. The disposal requirements adopted for the Guidelines should apply to both "consumer information" and "customer information".

4. Section III of the Guidelines should apply to the all disposal requirements applicable to "consumer information" and "customer information".

5. 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 institution's information security program".

Respectfully submitted,

ARMA International

By:

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

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