UNITED STATES OF AMERICA
Before the Federal Trade Commission

In the Matter of
The FACT Act Disposal Rule, R-411007

COMMENTS OF ARMA INTERNATIONAL
The Association for Information Management Professionals

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, hospital administrators, legal administrators, 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 strategy. 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 retention and disposition program for records of information, in the instance of this proposed rule, consumer information, 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.

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.

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.

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 articulated in an organization's formal, written information retention and disposition 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 maintained – 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 the training of employees of a covered organization, appropriate controls of the disposition and disposal of information, 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 records and information involved.

ARMA's comments are 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[1]" provides: "Records systems should be capable of facilitating and implementing decisions on the retention and

[1] 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

disposition of records. 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."

III. ARMA Comments to Proposed Section 682.2 Purpose and Scope.

A. *Purpose. This part implements section 216 of the Fair and Accurate Credit Transactions Act of 2003, which is designed to reduce the risk of consumer fraud and related harms, including theft, created by improper disposal of consumer information.*

The Commission properly articulates a goal of reducing the risk of consumer fraud and related harms created by improper disposal of consumer information.

To fully and completely safeguard against the "improper disposal of consumer information," disposal procedures should be incorporated into an organization's formal, written information retention and disposition program. The procedures adopted should include employee training, appropriate control mechanisms, and documentation of the disposal of the covered consumer information.

---

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."

B. *Scope. This rule applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information or any compilation of consumer information.*

The Commission properly proposes to apply this rule to any person within the Commission's jurisdiction that for a business purpose maintains or otherwise possesses consumer information.

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 managed according to a formal, written information retention and disposition program. This should not impose a burden on the organization; 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.

Compliance with legal and regulatory requirements is a key aspect of the role of a retention and disposition program within the context of an organization's business model and practices.

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 supports the application of this rule to any organization that possesses or otherwise accesses and processes consumer information.

IV. ARMA Comments to Proposed Section 682.3 Proper Disposal of Consumer Information.

A. *Standard. Any person who maintains or otherwise possesses consumer information, or any compilation of consumer information, for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.*

The Commission proposes to require a covered person, entity or organization to properly dispose of any consumer information it maintains or otherwise possesses by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

The proper disposal of any information vital to an organization's business interests must be guided by a formal, written information retention and disposition program, which will include a document destruction schedule, and the documentation that such records or other information were destroyed based on the identified life cycle of the information and in compliance to applicable laws and regulations.

Documentation of Disposition and Disposal

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 program, provides a threshold level of evidence for oversight and enforcement of the proposed rule.

ISO 15489-1 Clause 5, "Regulatory environment," provides: "All organizations need to identify the regulatory environment that affects their activities and requirements to document their activities. 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."

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."

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."

Reasonable Measures

Reasonable measures, based on recognized practices in information management, will include the adoption of a formal retention and disposition program, which in the case of consumer information within the stated purposes of this proposed rule, must include identification of the methodology of destruction that meets any promulgated rule, and the appropriate documentation that the identified methodology was engaged.

Draft Standard, Section 10 provides guidance for the development of disposition procedures, including policy considerations for disposition and destruction, suspension from disposition (primarily to address the event of pending or actual litigation or investigation, and verification of recorded information to be dispositioned.

Draft Standard, Section 10.4 provides specific guidance for "properly disposing" of information:

> 10.4. Destruction of Recorded Information. 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 strongly recommends that the Commission include in its rule a requirement that any covered person, entity, or organization adopt a formal, written information retention and disposition program for the covered consumer information that must include a document destruction schedule and appropriate documentation of the destruction of covered information.

B. *Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal …*

The Commission proposes examples intended to provide guidance on disposal measures that would be deemed reasonable under the proposed rule.

"In determining what measures are 'reasonable' under the Rule, the Commission expects that entities covered by the proposed Rule would consider the sensitivity of the consumer information, the nature and size of the entity's operations, the costs and benefits of different disposal methods, and relevant technology changes. 'Reasonable measures' are very likely to require elements such as the establishment of policies and procedures governing disposal, as well as appropriate employee training."

While the Commission articulates what is close to the recognition of an information retention and disposition program, just as it has done within the context of its Safeguards Rule, the proposed rule fails to clearly define this concept. Nothing in Proposed Section 682.3, neither (a) nor (b), requires in the case of the proposed rule, or recommends, in the case of the proposed codified examples, formally adopted written policies and procedures.

ARMA believes that reasonable measures must include formally adopted, written policies and procedures, in the form of a larger program of managing information within the organization, as articulated by a formally adopted retention and disposition program.

These policies and procedures, when acknowledged as formal, written requirements as part of the business practices of the organization, will better ensure compliance, will provide a source of training for employees and personnel responsible for the management of consumer information covered by this proposed rule, and will enable more meaningful enforcement for the Commission if and when an entity is suspected of or charged with impermissible practices.

ARMA agrees with the Commission's commentary that training will require "appropriate employee training". 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."

A properly implemented records retention program, with appropriate control mechanisms and assignment of responsibility, will also ensure upper management support and responsibility regarding the stewardship of the information covered by this proposed rule. The ARMA 1986 Guide provides that upper 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."

Requiring a formal written procedure for information management is not only consistent with established business practices, but is also consistent with the Commission's Safeguards Rule promulgated pursuant to the requirements of the Gramm-Leach-Bliley Act. See FTC Safeguards Rule at 16 CFR part 314.

The Safeguards Rule requires covered entities "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue." See Section 314.3 (Standards for safeguarding customer information).

The Rule includes specific elements that must insure the security and confidentiality of customer information, protect against any anticipated threats to the security or integrity of

such information, and protect against unauthorized access to or use of such information. See Section 314.3. Section 314.4 of the Rule requires the designation of employees for management and coordination, employee training, oversight of service providers, and evaluation and adjustment of programs, among other things.

V. ARMA Recommendations.

ARMA recommends the following required elements, consistent with the standards and guidelines of information management discussed above, be adopted as part of the proposed rule –

1. Covered organizations must formally adopt a written records retention and disposition policy for the covered consumer information. There should be evidence of upper management's endorsement of the program, with policies and procedures to ensure that necessary training and resources are available to ensure proper implementation. The program should also include regularly scheduled audits to determine compliance.

2. The management of information by covered organizations must document "cradle to grave" management of the covered consumer information, clearly documenting all disposition actions taken. Specifically, documentation of the disposal of the covered consumer information must be required.

3. The documentation of the organization's disposition and disposal of the covered consumer information must be maintained for a specified period of time, accessible within a reasonable period of time and in a format to ensure preservation and accessibility to ensure the ability of the Commission to provide necessary oversight and enforcement.

4. Employees of a covered organization, who are responsible for the use and management of the covered consumer information, must be appropriately trained in the retention and disposition program.

5. Proper control mechanisms must be implemented to ensure compliance with the retention and disposition program as it relates to the covered consumer information.

6. ARMA further recommends the development of specific elements, rather than the proposed examples, to ensure the proper policies and procedures are in place in a covered organization to ensure the proper destruction of the covered consumer information. The ARMA Draft Standard Section 10.4 would represent an appropriate guide, with sufficient flexibility, to enable any covered organization to develop a destruction schedule for the covered information within its larger information retention and disposition program.

Respectfully submitted,

ARMA International

By:

Juanita M. Skillman, CRM, FAI
Its Chairman of the Board and Immediate Past President
ARMA International
13725 West 109th Street, Suite 101
Lenexa, KS 66215
(888) 298-8219

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