

FACTA DISPOSAL RULE COMPLIANCE

AN EXECUTIVE GUIDE



FACTA Overview

In December, 2003, the federal government passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), a new law that affects various aspects of consumer credit.

Under FACTA, certain federal agencies were required to create regulations designed to minimize the risk of identity theft and consumer fraud by enforcing the proper destruction of consumer information. One of the resulting regulations, known as the Disposal Rule, was issued by the Federal Trade Commission in November 2004. Identical rules adopted by the federal banking agencies and the Securities and Exchange Commission now apply to organizations regulated under their authority.

Effective June 1, 2005, the Disposal Rule states that “any person who maintains or otherwise possesses consumer information for a business purpose” is required to properly dispose of the information, whether in electronic or paper form, by “taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.”

This document is provided as a courtesy by Iron Mountain. The material inside is offered as an overview of the new FACTA legislation and is subject to change without notice. Those with specific questions about the FACTA Disposal Rule should please contact the U.S. Federal Trade Commission.

The New FACTA Disposal Rule: Is Your Company Compliant?

In 2004, nearly 70% of all identity thefts occurred **offline***. The reason? Lack of proper information disposal and inadequate document shredding programs within organizations.

To address the responsibility of businesses to better police their procedures for destroying personal information, the federal government enacted the **Disposal Rule, effective June 1st, 2005**. This broad regulation impacts all U.S. businesses regardless of size or industry that possess consumer information. The regulation ***defines acceptable methods of consumer information disposal and assigns penalties when a company is non-compliant.***

Under the Disposal Rule, businesses are now compelled to assess the effectiveness of security procedures related to information disposal to meet federal compliance guidelines. Failure to do so can have grave consequences.

- Does your company have an information destruction policy in place to meet the Disposal Rule requirements?
- Are you taking the steps necessary to rapidly ensure federal compliance?
- If not, you may be exposing your customers, your company and your employees to tremendous liability.

As the industry leader in records and information management, Iron Mountain has prepared a brief Disposal Rule overview to help you understand its implications and take the necessary steps to ensure compliance.

*Javelin Strategy & Research, Copyright 2004, Pleasanton, CA

The Disposal Rule: What It Says

The Disposal Rule requires “any person or company who maintains or otherwise possesses consumer information to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.” “Consumer information” is defined as any record about an individual that is a consumer report, or is derived from a consumer report, including compilations of such records.

What It Means by “Reasonable Measures”

Disposal Rule compliance cannot be achieved by relying on a personal shredder under a desk. Nor can your janitorial staff or your landlord be expected to properly destroy critical data. Today, a secure, proven system of records disposal is legally required if your records contain consumer information.

Here are two examples the FTC has given of destruction techniques that would constitute “reasonable measures” taken to protect against unauthorized access or use of consumer information:

- 1) Burning, pulverizing or shredding of information
- 2) Destruction or erasure of electronic media so that information cannot be read or reconstructed

However, focusing only on physical document destruction does not go far enough. Companies must create, and abide by, well-defined policies and procedures governing what information gets destroyed and how. A clear and effective employee communications program discussing what to do and why is required. Without these policies, information disposal bins lying around the copy room will be meaningless and companies will risk the dangers associated with non-compliance. In addition, if companies elect to use a third-party shredding service provider, the Disposal Rule requires them to exercise due diligence in making sure the service provider’s procedures keep records secure during the disposal process. Also, after the service contract is signed, companies must monitor their service provider’s performance to make sure it meets contractual requirements.

What are the Costs of Non-Compliance?

The new Disposal Rule impacts every business that operates in the United States, from financial organizations to entertainment studios; national retailers to local law firms; securities firms to landlords. To ignore or fail to fully comply with the law exposes you and your company to very serious risk.

Irreparable damage to your corporate reputation.

For most companies, this is by far the greatest liability. If charged with non-compliance, your company could also risk:

- Loss of investor confidence and shareholder value
- Loss of revenue, market share and customers

Other costs of non-compliance:

- Significant fines
- Expensive litigation that drains precious capital, time and productivity

How Can Your Company Become FACTA Compliant?

Companies already governed by industry specific legislation, such as HIPAA and the Gramm-Leach-Bliley Act, cannot become complacent. They too must review internal policies and procedures to ensure Disposal Rule compliance.

Disposal Rule compliance demands the design and implementation of new, stricter policies that better manage how consumer information flows from your employees to its final, non-recoverable form. How does the information get created? How does it move within your organization? How does it get removed from your site? How does it get destroyed?

The compliance solution you select must ensure that security principles are applied throughout all phases of the information's life cycle. One weak link could jeopardize your whole program. Steps you must take include:

- Create or modify existing policies regarding the disposal of consumer information
- Identify any new procedures, training and involvement of necessary personnel
- Select, after investigation, an appropriate information management partner if needed
- Establish service agreements with this partner that specify frequent monitoring of procedures to ensure on-going compliance
- Educate and train employees
- Audit the process to identify "weak links" or performance gaps

How Do You Build a Compliant Program?

Today's challenge is to develop a defensible program that clearly shows the "reasonable measures" a company has taken to manage and demonstrate compliance. Keys to creating this type of successful program include:

- **Reasonable Measures.** The Disposal Rule does not define "reasonable measures," although it furnishes examples of what constitute reasonable measures. Until the FTC expands upon the definition of "reasonable measures," companies have an ongoing duty to protect all consumer information during the disposal process. Other laws and regulations set requirements for security of personal information prior to disposal for many industries.
- **Consistent disposal practices and procedures company-wide that establish a standardized approach to compliance.**
- **Management accountability: maintaining an unbroken chain of custody.** This ensures the highest level of security, from the moment the information is created until its disposal. Remember, one weak link can jeopardize your entire program.
- **Employee adoption.** Employees should understand how to comply and should have the knowledge to make decisions in the best interest of your company.
- **An efficient and cost-effective program.** Information should be stored and disposed of with consideration for your company's workflow, workforce and workplace environment.
- **Minimal organizational impact.** Implementation of compliance policies should be transparent and non-disruptive.
- **An ability to measure the success of your compliance program.** This allows for correction of any failure points or modifications as changes in work patterns, work force and new laws require.

Depending on the nature and size of your company, the sensitivity of the information held and the costs/benefits of different disposal methods, your compliance solution could be as simple as instituting a few basic in-house procedures. However, for most companies, a more secure alternative — and one the FTC recognizes — is to contract with a reputable information management and destruction partner who can rapidly and effectively implement a program consistent with the various requirements of the new rule.

Why Iron Mountain?

For over 50 years, Iron Mountain has been the world leader in records and information management. Today, our team of experienced, knowledgeable professionals can offer your company a Disposal Rule-compliant Secure Shredding Program that will quickly and cost-effectively help you meet compliance requirements. It is available at no extra charge to businesses that outsource their shredding programs with us. As your information management partner, we will work with your organization to:

- Create new policies or modify your existing ones regarding the disposal of confidential and consumer information
- Identify any new procedures or necessary training and determine what key personnel need to be involved
- Assist in the implementation of all new policies and procedures
- Provide a written contract as to what steps will be taken during the destruction process to ensure compliance
- Constantly monitor program adherence and effectiveness
- Provide compliance monitoring procedures your own employees can follow
- Develop education and training materials to help guide your employees in performing these duties

How Iron Mountain Can Help You Transform Your Records Management Program into a Compliance Program

At Iron Mountain, we don't approach disposal as a separate program but as the final stage of a larger, more encompassing Compliant Records Management program. Based on our experience working with hundreds of large corporations, we strongly recommend the following six-stage approach for company-wide consistency, accountability, adoption and accessibility:

Organize — Gain executive level support of the program and assign a program manager to delegate departmental responsibilities.

Assess — Evaluate existing disposal procedures, define new Disposal Rule requirements and determine necessary actions.

Develop — Create or modify your existing program with the partner you have selected to ensure your disposal procedures are in compliance with the Disposal Rule.

Implement — With the help of your secure shredding partner, send advanced communications to managers in all offices affected by the new Rule and roll out your program company-wide.

Manage — Regularly review reports that identify gaps in your plan that could increase risks and costs.

Audit — Conduct a formal examination of your FACTA program to remain compliant and ensure top-level accountability.

Given the challenges of today's heavily regulated environment, companies must choose a partner they trust to store, manage and safeguard their valuable information assets. With incomparable service, resources and leading edge technologies, Iron Mountain will provide you with a comprehensive, cost-effective records management solution that will protect your customers, and your business, from risk and exposure.

To learn more about FACTA Disposal Rule compliance, please contact us at (800) 899-IRON or visit us at www.ironmountain.com.

The Federal Trade Commission

16 CFR Part 682

Final Rule: Disposal of Consumer Report Information and Records

Sec.

682.1 Definitions.

682.2 Purpose and scope.

682.3 Proper disposal of consumer information.

682.4 Relation to other laws.

682.5 Effective date.

Authority: Pub. L. 108-159, sec.216.

§ 682.1 Definitions.

(a) In general. Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.

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

(c) “Dispose, disposing or disposal means:”

1. the discarding or abandonment of consumer information, or
2. the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.

§ 682.2 Purpose and scope.

(a) Purpose. This part (“rule”) 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 identity theft, created by Improper disposal of consumer information.

(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.

§ 682.3 Proper disposal of consumer information.

(a) Standard. Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measure to protect against unauthorized access to or use of the information on connection with its disposal.

(b) Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with this rule

- (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of paper containing consumer information so that the information cannot practically be read or reconstructed.
- (2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practically be read or reconstructed.
- (3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.
- (4) For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (1) and (2) above.
- (5) For persons subject to the Gramm-Leach-Bliley Act, 15 U.S.C. 6081 et seq., and the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR 314 ("Safeguards Rule"), incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.

§ 682.4 Relation to other laws.

Nothing in this rule shall be construed:

- (a) To require a person to maintain or destroy any record pertaining to a consumer that is not imposed under other law; or
- (b) To alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

§ 682.5 Effective date.

This rule is effective on June 1, 2005.

By direction of the Commission.

About Iron Mountain

Iron Mountain Incorporated (NYSE:IRM) is the world's trusted partner for records management and data protection services. Founded in 1951, the Company has grown to service more than 235,000 customer accounts throughout the United States, Canada, Europe and Latin America. Iron Mountain offers records management services for both physical and digital media, disaster recovery support services, and consulting — services that help businesses save money and manage risks associated with legal and regulatory compliance, protection of vital assets, and business continuity challenges. For more information, visit the Company's Web site at www.ironmountain.com.

IRON MOUNTAIN SERVICES



RECORDS MANAGEMENT

Iron Mountain provides compliant records management solutions to manage and protect your information assets. Our records management programs ensure that your business records are secure and easily accessible. We offer specialized services tailored to your unique needs.



SECURE SHREDDING

Given the confidential nature of business records, it's important to ensure complete destruction. Our secure shredding services help you to protect the privacy of your company, employees and customers.



DIGITAL ARCHIVES

Our Digital Archives service group offers compliance and records management solutions for today's leading organizations. We provide SEC-compliant digital archiving, supervision and data restoration and electronic discovery support services. With our extensive records management expertise we can help institute a comprehensive and compliant records management solution.



DATA PROTECTION

Whether physically transporting and vaulting your backup tapes at one of our secure facilities or backing up your data through a secure Internet connection with Electronic Vaulting, our comprehensive data protection and disaster recovery services place your information off-site, off-line and out-of-reach; yet the data is accessible whenever and wherever you need it.



VITAL BUSINESS RECORDS

Our climate-controlled, secure facilities are designed to protect irreplaceable documents like original deeds, wills, trusts, contracts, patents, and other notarized and certified records for you.



CONSULTING

Today's business world demands that companies follow sound, consistently applied records management practices. Let our consulting professionals review your current records management program, help you determine which records you need to retain, and create an appropriate retention schedule and records classification program for each.

© 2005 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, and Latin America. For more information, visit our Web site at www.ironmountain.com