



**Back Thru
The Future**

**Technology
Disposal**

Environmental Excellence for 20 Years.

Are you ready for the new
RED FLAG RULE
*and its impact on your
technology disposal practices?*

Daniel F. Bayha, Vice President

Back Thru The Future Technology Disposal
150 Main Street
Ogdensburg, NJ 07439
973-823-9752
shred@backthruthefuture.com

November 11, 2009

The Federal Trade Commission's new Red Flag Rule is scheduled to go into effect June 1st 2010.

The rule will require that all financial institutions and others who are considered "creditors" must:

1. Identify in writing the areas of their operation where the personal information of their clients is at risk of unauthorized access;
2. Develop written procedures to mitigate that risk;
3. Detect unauthorized access if or when it happens.

This new rule will be appended to the existing financial services regulations: GLB, FCRA, and FACTA.

It is important to understand that sensitive personal information stored on to be disposed of electronic media has already been identified within the above acts as a data security risk area and specifically addressed under the "FACTA Disposal Rule". The FACTA disposal rule under statute has been appended to GLB.



The FACTA Disposal Rule states:

Any person who maintains or otherwise possesses 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.



What constitutes "disposal"?

Routine destruction of the records or information is included, but the rule also includes "abandonment of consumer information" and "the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored." 16 C.F.R. § 682.1(c). Thus, organizations must be concerned not only with routine document retention and destruction policies and procedures covering consumer information, but also policies and procedures related to the transfer, donation, or other disposition of computer equipment and other media on which consumer information may be located.

Companies must also concern themselves with the method of destruction.

The rule "does not mandate specific disposal measures," and the FTC's commentary specifically notes that appropriate methods will often depend on the affected companies resources.

The issue of appropriate destruction methods has recently become more clearly defined by the issuance by the National Institute of Standards and Technologies (NIST) Special Publication 800-88 "Guidelines for Media Sanitization". This publication has been referenced as the guideline for destroying data under the new (Sept 23, 2009) HITECH "Data Breach Notification" provisions of HIPAA.

What are "reasonable measures"?

The FTC offers several examples addressing specific methodologies. In addition to acknowledging accepted methods of document destruction, including "burning, pulverizing, or shredding of papers," and "destruction or erasure of electronic media," the Commission specifically addressed the relationship and responsibilities of record owners and data destruction service providers. The record owner must "take reasonable steps" to select and retain a service provider that is capable of properly disposing of the consumer information at issue. Finally, the Commission emphasizes that "'reasonable measures' require the establishment of written policies and procedures governing disposal, as well as appropriate employee training."

Conclusion:

The new Red Flag Rule further emphasizes our government's concern with the protection of personally sensitive information and the ongoing tightening of the responsibilities and expansion of the liabilities of organizations handling this type of information. Destroying sensitive information contained on to be disposed of data media has been specifically identified as an area of concern. Written policies concerning the destruction of this type of data need to be developed and, if written policies already exist, reviewed in light of the specific requirements of these new regulations. NIST publication 800-88 is rapidly emerging as the recognized legal and regulatory standard for the approved destruction of this type of data. Utilizing a third party to destroy sensitive data requires that an organization does the appropriate "due diligence" of the third party's capabilities and that the third party be able to provide auditable proof of their adherence to the NIST standards. Willful or even negligent failure to comply with the new rules could subject covered entities to civil liabilities and penalties.