Long delayed, enforcement of the Fair and Accurate Credit Transaction Act (FACTA) Red Flags Rule finally began in January 2011. With this regulation in effect, it’s no longer enough to ensure the proper disposal of sensitive information. Now, businesses of all kinds are required to create and put in place a written Identity Theft Prevention Program – and can suffer civil penalties and injunctions if found to be in noncompliance.

**What’s in it.**
The Red Flags Rule spells out what compliance is – essentially, what needs to go into the written plan. With a reasonable plan in place, companies should be able to:

- Identify the so-called “red flags” – patterns and activities that may indicate the presence of identity theft
- Build methods for detecting red flags into standard business practices
- Document all responses taken in reaction to signs of potential identity theft
- Update the plan over time to stay current with evolving risk factors

Fortunately, the Red Flags Rule “includes guidelines to help financial institutions and creditors develop and implement a Program, including a supplement that offers examples of red flags.”

**Who should pay attention.**
As with FACTA itself, the Red Flags Rule has implications for organizations of all sizes and kinds.

Broadly, it covers two categories of businesses: “financial institutions” and “creditors.” The definition of “financial institution” is relatively straightforward:

- All banks, savings associations, and credit unions, regardless of whether they hold a transaction account belonging to a consumer; and
- Anyone else who directly or indirectly holds a transaction account belonging to a consumer.

As for “creditors,” that term covers a lot of ground. Inclusion is based on three general criteria. Creditors:

- Obtain or use consumer reports in connection with a credit transaction;
- Furnish information to consumer reporting agencies in connection with a credit transaction; or
- Advance funds to – or on behalf of – someone, except for funds for expenses incidental to a service provided by the creditor to that person.

Last-minute changes to the rule somewhat limited the scope of what constitutes a “creditor,” but to date there are no hard-and-fast guidelines for which businesses fall under the rule and which don’t. According to the Federal Trade Commission, “Examples of groups that may fall within this definition are utilities, health care providers, lawyers, accountants, and other professionals, and telecommunications companies.” But the rule could theoretically cover any company (or person) that provides a product or service at a given time and accepts payment for it at a later date.

If that’s not confusing enough, the rule only comes into play if an organization holds consumer accounts “designed to permit multiple payments or transactions – or any other account for which there is a reasonably foreseeable risk of identity theft.”

**How to comply.**
Because of the Red Flags Rule’s complexity and recent implementation, it’s best to consult an attorney to see if your organization falls under its jurisdiction. You can also search the FTC website for information on the rule and guidelines on creating an Identity Theft Prevention Program.

Let A Shred Ahead help you comply with Federal regulations.

Using state-of-the-art shredding equipment, A Shred Ahead provides secure shredding services for businesses and government agencies. A Shred Ahead destroys all types of confidential and sensitive information, including financial records, electronic media, medical records, and intellectual property.

We help companies institute programs designed to comply with state and federal regulations. Let us do the same for you.

Visit us online at www.ashredahead.com or call us at 866.933.7171 to request a quote or additional information.