



Report Content Writer
www.reportcontentwriter.com.

AUTHOR: Rachel Agheyisi

EMAIL: rachel@reportcontentwriter.com.

TWITTER: www.twitter.com/rachel_rcw.

The Fight against Identity Theft – The Red Flags Rule

Identity theft continues to pose a threat to U.S. consumers. The latest report released by the Federal Trade Commission (FTC) in February 2009, showed that, for the ninth year in a row, identity theft topped the list of consumer complaints filed with the Commission. Additionally, the report showed that credit card fraud was the most common form of reported identity theft. It is therefore no surprise that additional safety measures are needed to protect consumers.

The latest tool in the fight against identity theft is the implementation of section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act or FACTA). Section 114 involves the issuance of the Red Flags Rule enforced by the FTC, the federal bank regulatory agencies, and the National Credit Union Administration (NCUA).

This article highlights the Red Flags Rule, including its definition, compliance requirements, and enforcement date.

What is the Red Flags Rule?

The Rule requires many businesses and organizations to implement a written *Identity Theft Prevention Program* (the Program) designed to detect the warning signs of identity theft in their day-to-day operations. These warning signs are referred to as "**red flags**". The Program should be designed to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.

The Red Flags Rule focuses on credit transactions because these are the types of transactions most easily exploited by identity thieves. Identity thieves tend to look for opportunities to obtain products or services that do not require up-front payment.

Does the Red Flags Rule apply to your business?

According to the final rules published by the regulatory agencies, only those **creditors** and **financial institutions** that offer or maintain "**covered accounts**" must develop and implement a written Program.

Determining whether the Rule applies to your business hinges on examining the legal definitions of three concepts:

1. Creditor
2. Financial institution
3. Covered account

1. Who is a creditor?

The FACTA's definition of "creditor" includes any business entity that regularly extends or renews credit – or arranges for others to do so – and includes all entities that regularly permit deferred payments for goods or services.

Some examples of creditors are:

- finance companies;
- automobile dealers that provide or arrange financing;
- mortgage brokers;
- utility companies;
- telecommunications companies;
- non-profit and government entities that defer payment for goods or services; and
- businesses that provide services and bill later, including many lawyers, doctors, and other professionals.

2. What is a financial institution?

FACTA'S definition of financial institutions includes entities that offer accounts that enable consumers to write checks or make payments to third parties through other means, such as other negotiable instruments or telephone transfers. Examples include a state or national bank, a state or federal savings and loan association, a mutual savings bank, and a state or federal credit union.

3. What is a covered account?

According to the final guidelines, a covered account is meets one of these two criteria:

1. An account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or
2. Any other account for which there is a reasonably foreseeable risk of identity theft for customers, or the safety and soundness of the financial institution or creditor.

Each financial institution and creditor must periodically determine whether it offers or maintains a "covered account."

What are the key elements of the written Program?

The Red Flags Rule gives covered businesses the flexibility to design an Identity Theft Prevention Program (the Program) appropriate for the business, given its size and potential risk for identity theft.

However, the final regulations list the four basic elements that must be included in the written Program of a financial institution or creditor.

The compliant Program must contain “*reasonable policies and procedures*” to:

1. Identify relevant red flags for covered accounts and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers, financial institution or creditor from identity theft.

A caveat based on risk level

While some companies need a comprehensive Program, the final rules made provision for businesses and organizations deemed at low risk for identity theft. For example, businesses that know their customers personally may have a low risk of identity theft. These entities may adopt a streamlined Program to comply with the law.

On May 13, 2009, the FTC announced that it had created a template for use in developing a streamlined Program. The template includes guidance and instructions that enable companies to complete and print the fill-in-the-blank form online. It is available at the FTC website: www.ftc.gov.

FTC Enforcement Date

On April 30, 2009, the FTC announced that it had delayed enforcement of the “Red Flags Rule” until **August 1, 2009** (from May 1, 2009), to give creditors and financial institutions under its jurisdiction more time to comply.

Summary - compliance in a 4-step process

The Red Flags Rule is one more tool in the continuing effort to safeguard consumer personal information. Compliance is a four-step process that involves: 1) identifying relevant red flags (warning signs), 2) detecting red flags, 3) preventing and mitigating identity theft, and 4) maintaining an updated Program.

For more information, visit the FTC website at www.ftc.gov.

About the Author: Rachel Agheyisi is a business writer who specializes in white papers and case studies that address regulatory compliance and business intelligence issues. Related articles are available on her website at www.reportcontentwriter.com.