

# FTC Delays Enforcement of Red Flags Rule Through December 31, 2010 To Give Congress Time To Exempt Certain Businesses From Rule's Requirements

May 28, 2010

---

SECURITY & PRIVACY ALERT - MAY 28, 2010

---

written by [Gabriel M. Helmer](#)

This morning, Friday, May 28, 2010, the Federal Trade Commission (FTC) [announced](#) that it was extending the deadline for enforcement of the Red Flags Rule through December 31, 2010, in order to give Congress sufficient time to amend the law to exclude certain businesses from application of the Rule.

In October 2009, the FTC delayed its enforcement of the Red Flags Rule in response to the U.S. House of Representatives unanimous passage of [H.R. 3763](#), a bill that would exclude from coverage of the Rule all law firms, accounting firms and medical practices with 20 or fewer employees. This week, Senators Thune (R-SD) and Begich (D-AK) introduced [S. 3416](#), a parallel bill, in the Senate. When announcing the new deadline, the FTC urged Congress "to act quickly to pass legislation that will resolve any questions as to which entities are covered by the Rule and obviate the need for further enforcement delays."

The FTC, Federal Reserve, FDIC and other federal regulatory authorities adopted the Red Flags Rules in January 2008 in response to the enactment of the Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681. The Rules have been in effect for banks, credit card companies and traditional financial institutions since November 1, 2008. However, there have been delays in enforcement of the FTC's Red Flags Rule, as set forth in 16 C.F.R. Part 681, which apply more broadly to "creditors."

In 2008, the FTC caused considerable controversy by construing the term "creditor" to apply to any business that sells goods or services now and bills its customers later, including doctors, lawyers and many other businesses. In response to the FTC's broad interpretation, groups representing the legal, accounting and medical industries have filed lawsuits to prevent the FTC from enforcing the Red Flags Rule against their constituents.

In general, the Rule requires that affected businesses perform a routine self-assessment to determine whether it maintains any kind of "covered account" that creates a reasonably foreseeable risk of identity theft. This would include a consumer account such as those maintained by a utility company or cell phone provider or a wide range of accounts that permit multiple customer transactions.

Businesses that are subject to the Red Flags Rule and maintain covered accounts must develop a written identity theft prevention program to detect the warning signs or "Red Flags" of identity theft and mitigate the potential harm to consumers. The basic elements of a compliant identity theft prevention program include:

- The appointment of a identity theft / information security coordinator
- Procedures to identify Red Flags, warning signs and security risks
- Procedures for responding to Red Flags that have been detected
- An effective training program to educate staff on how to recognize and respond to Red Flags
- Ongoing oversight and monitoring of the identity theft prevention program.

For more news and analysis of the FTC Red Flags Regulations, please visit the forum developed by Foley Hoag's Security & Privacy Practice Group at [www.SecurityPrivacyandtheLaw.com](http://www.SecurityPrivacyandtheLaw.com) and the [FTC's Red Flags Rules website](#). Foley Hoag is advising clients developing information security programs in compliance with the Red Flags Rules, Massachusetts identity theft regulations, as well as other federal, state and international laws regarding information security and identity theft.