FICAP eNEWS

# Red Flags Rule

Bennett Acuff

Time is running out to understand, implement, and comply with the Federal Trade Commission's (FTC) "Red Flags Rule," 16 C.F.R. § 681.2. Although the FTC has delayed the compliance date four times (originally scheduled for November 1, 2008), it appears the June 1, 2010 deadline is set in stone. The Red Flags Rule will apply to a wide array of business organizations and understanding compliance requirements is vital. But what is the purpose of the Rule and how will businesses comply?

**Purpose:**

The Red Flags Rule is a set of regulations implemented by the FTC to tackle the escalating problem of identity theft, by requiring certain entities to create and implement policies and procedures to safeguard individual consumers and businesses.

The FTC issued the Red Flags Rule in November 2007 requiring businesses and organizations to implement a written "Identify Theft Prevention Program" designed to detect the warning signs of identity theft. The Rule applies to financial institutions and creditors who have "covered accounts." The House of Representatives recently passed a bill exempting health care providers, accounting and law firms.

A creditor is defined as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit." If a business is a creditor, it must also determine if it has any "covered accounts." Pursuant to the Rule, there are two different kinds of "covered accounts":

A. A consumer account a business offers customers that's primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions; and

B. Any other account that a creditor offers or maintains for which there is a foreseeable risk to customers or creditor from identify theft, including financial, operational, compliance, reputation, or litigation risks.

(Examples include small business accounts and single transaction consumer accounts that may be vulnerable to identity theft).

If a business is a creditor and has “covered accounts,” it must have a written program. The Rule sets out four steps to develop, implement and administer an Identity Theft Prevention Program:

1) The Program must include “reasonable” policies and procedures to identify the “red flags.” (“Reasonable” will be determined based on the size and nature of the business);
2) The Program must be designed to detect the red flags that have been identified. (For example, if you have identified fake addresses as a red flag, you must have procedures in place to detect possible fake addresses);
3) The program must spell out appropriate actions you will take when you detect red flags;
4) The program must be periodically re-evaluated.

It is very important for a business to understand and comply with the Red Flags Rule.

While guides, like the C.F.R., are administrative interpretations of the law—and do not have the full force and effect of the law—failure to comply with the Rule could lead to corrective action by the FTC, and resulting civil penalties.

*For further information on how to comply with the Red Flags Rule, please contact Bennett Acuff, at Hill Will Henderson, P.A.*