



In November, 2007, the Federal Trade Commission (FTC) enacted regulations, commonly referred to as the “Red Flags Rule” (“RFR”). RFR requires financial institutions and creditors to implement written programs for detection of misuse of identifiable personal information to commit identity theft. RFR becomes effective June 1, 2010. Failure to comply may result in a number of administrative and civil penalties, described below.



### Who Is Covered?

RFR applies to:

- Financial institutions; and
- “Creditors” with “Covered Accounts”

While the meaning of a “*financial institution*” includes banks, credit unions, the definition of a “*creditor*” is less obvious.

RFR defines a “*creditor*” as any entity that regularly extends or even simply arranges for the extension of credit. Thus, swept in the net of the “*creditor*” definition is a vast majority of businesses not requiring full payment at the time of provision of goods/services. Such businesses include, for example, mortgage brokers, law firms, and even non-profit institutions that permit payment over time. This equally affects home builders given services like pre-qualification of buyers and in-house mortgage brokerage.

Accounts evidencing partial or extended payments are largely included in the definition of “*covered accounts*,” i.e., accounts (i) involving or are designed to permit multiple payments/transactions; or (ii) having a reasonably foreseeable risk for identity theft. As a result, RFR covers most billing accounts, including credit cards, mobile phone accounts and business accounts.

### Dealing With Red Flags

RFR mandates that each covered business implement a written program to detect and respond to patterns, practices or specific activities (known as “red flags”) that indicate possible identity theft. The nature of “red flags” depends on the business. For example, a credit card issuer could notice an unusual level of purchases while commercial builders should be wary of contract signatures that do not match the identification documents.

Some common “red flags” are:

- Forged documents;
- Non-matching signatures;

- Address discrepancies;
- Complaints from customers for services never ordered;
- Fraud alerts from credit reporting agencies.

To ensure detection businesses must implement written programs customized to detect, address, mitigate and prevent the identity theft risks. The plan must provide for staff training and service provider supervision. Further, the plan must outline the mechanics of future updates. Such program should be managed by a board of directors/equivalent management and supervised by senior officers.



Failure to comply with RFR may result in regulatory enforcement action, civil monetary penalties of up to \$3,500 per violation, and in certain cases up to \$16,000 per violation per day for continued non-compliance, statutory penalties of up to \$1,000 per injured individual, punitive damages and attorneys' fees. Additional detrimental consequences may include diversion of resources to deal with the FTC and loss of business.



Every company providing "credit" in the form of lending, leasing, or extended payments, should take steps to achieve compliance, including:

- immediate review of existing confidential information protection and history of identity theft incidents;
- development of a written program for detection, response, mitigation and prevention of identity theft;
- review and approval of such program by the company's board of directors/senior management;
- appointment of a senior officer in charge of the program;
- comprehensive training of employees handling confidential information;
- establishment of guidelines of supervising service providers having access to confidential information;
- establishment of process for regular updates to the program.

**rising Stars 40 under 40**