

## **The Red Flags Rule: Does It Apply To Your Business?**

**Barbara K. Letcher**  
**Newhouse, Prophater, Letcher & Moots, LLC**  
**5025 Arlington Centre Boulevard, Suite 400**  
**Columbus, Ohio 43220**  
**(614) 255-5441**  
[bletcher@nplmlaw.com](mailto:bletcher@nplmlaw.com)

On November 1, 2009, the Federal Trade Commission will begin enforcement of the Red Flags Rule which requires many businesses and organizations to implement a written Identity Theft Prevention Program to detect the warning signs of identity theft likely to surface in their day to day operations. Whether you are required to comply with the Red Flags Rule depends on whether your organization is a “financial institution” or “creditor” and whether it has “covered accounts”.

The Red Flags Rule defines a “financial institution” as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer. “Financial institutions” are those entities that offer accounts that allow consumers to write checks or make payments to third parties through other means such as telephone transfers or by way of other negotiable instruments.

The definition of “creditor” is much broader and includes those businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill customers later. Healthcare providers, utility companies, telecommunication companies and law firms are among the entities that may fall under this definition depending on how and when they collect payment for their services. A “creditor” can also be an entity that regularly grants loans, arranges for loans or an extension of credit, or makes credit decisions. Finance companies, mortgage brokers, real estate agents, automobile dealers, and retailers that offer financing or help consumers get financing from others by processing their credit applications would be among the types of businesses that would be considered “creditors”. If you regularly extend credit to other businesses, you may be considered a “creditor” for purposes of the Red Flags Rule. Finally, if your business regularly participates in the decision to extend, renew or continue credit, including setting the terms of credit, you may be a “creditor” subject to the Red Flags Rule.

Determining whether your business or organization is a “financial institution” or “creditor” does not end the inquiry. Once you conclude that your business or organization falls within the type of entity that may be covered, you must determine if you have any “covered accounts”. The Red Flags Rule only applies to entities with “covered accounts.” Both existing accounts and new accounts must be considered.

One type of a covered account is a consumer account provided to customers primarily for personal, family or household purposes that permits multiple payments or

transactions. These accounts are always “covered accounts” under the rule and include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts.

The second type of “covered account” is “any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.” Included within the scope of this second type of covered account are small business accounts, sole proprietorship accounts or single transaction consumer accounts that may be vulnerable to identity theft. These types of accounts are “covered accounts” only if the risk of identity theft is reasonably foreseeable.

If your business is a “financial institution” or “creditor” and has “covered accounts”, you must comply with the Red Flags Rule by implementing a written Identity Theft Prevention Program. If you do not have any “covered accounts”, a written program is not required. However, you should maintain a written record of your analysis of whether the Red Flags Rule applies to your business or organization for purposes of demonstrating compliance. In addition, a periodic assessment of both your accounts and the risk that may be associated with them must be done to determine whether you have acquired covered accounts which require compliance with the Red Flags Rule.

Finally, compliance is not optional. The FTC intends to enforce the Red Flags Rule and the consequences of noncompliance range from a civil monetary penalty for each violation to a regulatory enforcement action that will result in increased government oversight of your business. While the Red Flags Rule does not provide a mechanism for an individual to bring a legal action in the event of a violation, failure to comply may be evidence of a failure to meet a reasonable standard of care in a negligence action brought to recover damages for identity theft. The cost to your business for a data breach stemming from noncompliance extends beyond financial penalties. The cost will be reflected in the loss of trust of your customers when the confidential information with which you have been entrusted is placed in jeopardy.