

October 2009

LEGAL ALERT:

Red Flags Rule Requires Organizations to Implement a Program to Fight Identity Theft

The Federal Trade Commission (“FTC”) is now enforcing a “Red Flags Rule” that requires many businesses and organizations, including nonprofit entities, to implement a written Identity Theft Prevention Program. Identity theft is a fraud attempted or committed using identifying information of another person without authority. The Identity Theft Prevention Programs must be designed to detect and react to warning signs—or “red flags”—of identity theft in an organization’s day-to-day operations. The idea behind the rule is that, by identifying red flags in advance and considering how to respond, organizations and businesses will be better prepared and equipped to thwart identity theft problems when they do arise.

WHAT’s the Rule?

The Red Flags Rule says that “financial institutions” and “creditors” that hold any “covered account,” or other account for which there is a reasonably foreseeable risk of identity theft, must develop and implement an Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts.

WHOM Does This Rule Apply to?

The rule applies to “**financial institutions**” and “**creditors**” with “**covered accounts.**” Businesses and organizations that do not ordinarily consider themselves “financial institutions” or “creditors” must be careful because the definitions may sweep you in. It does not necessarily matter what line of work you are in; the definitions in the rule determine whether or not your organization or business is covered.

According to the rule, a “**financial institution**” is 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 entity that, directly or indirectly, holds an account from which a consumer can make payments or transfers to third parties. Examples of such accounts are checking accounts, savings deposits subject to automatic transfers, and share draft accounts.

“**Creditor**” is defined in broad terms under the rule, and captures many nonprofit groups and government agencies. The term includes businesses or organizations that regularly provide goods or services first and allow customers to pay later. For example, schools that bill for tuition after students attend class are creditors under the rule. Also included are entities that regularly grant or arrange for loans, or make credit decisions. Moreover, an entity that regularly arranges for the extension, renewal, or continuation of credit (to either individuals or to other businesses)

is a creditor, such as one that regularly collects or processes credit applications for third-party lenders. However, merely providing advertising brochures for third party financing, telling your customers about third party financing without referring them to lenders, or accepting credit cards as a method of payment, does not alone make an entity a “creditor.” Similarly, whether an entity pulls credit reports or collects personal information such as social security numbers is not relevant to determining whether the organization is covered by the rule. Collecting a retainer fee in advance of providing services does not make you a creditor either. The Rule applies to businesses that regularly defer payment until *after* services are provided.

If your organization fits within the definition of either “financial institution” or “creditor,” the next step is to determine whether you have any “**covered accounts**.” There are two types of covered accounts: (1) a consumer account you offer your customers that is primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions; and (2) any other account that you offer or maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of your entity from identity theft, including financial, operational, compliance, reputation, or litigation risks. Examples of the first category are credit card accounts, mortgage loans, cell phone accounts, and checking accounts. Examples of the second include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to identity theft. In determining whether your accounts fall into the second category, consider how they are opened and accessed. Business accounts that can be accessed remotely through the phone or internet, for example, may carry a reasonably foreseeable risk of identity theft. Note that even if your organization does not have any covered accounts now, you must check periodically if you are a financial institution or creditor. The details of this periodic reassessment must be part of your organization’s written Identity Theft Prevention Program.

HOW Do We Comply if Our Organization Falls Under the Rule?

Entities whose activities fall within the definition of “financial institution” or “creditor” and who have a “covered account” must develop a written program to identify and detect red flags for identity theft. The program can be tailored to suit the size, complexity, and risk level of your organization. Operations carrying a low risk of identity theft, for example, may only require a streamlined program, while a more complex organization with a higher risk of identity theft may need a much more comprehensive one. Your organization’s board of directors, or a committee of the board of directors, must approve your first written program. If you do not have a board, an appropriate senior-level employee should determine approval.

The program first must include reasonable policies and procedures to identify the “red flags” of identity theft that you may encounter in the day-to-day operations of your business. Red flags are suspicious patterns, practices or activities that should call your attention to the possibility of identity theft. For example, if a customer has to provide identification to open an account with your organization and the ID looks fake, that would be a red flag for your business. Second, the program must be designed to detect these red flags that you have already identified. For example, there should be procedures in place to detect possible fake, forged or altered identification if fake IDs are an identified risk for your organization. Third, the program should detail the appropriate responses that your business should take in the event a red flag is detected. The responses should aim to prevent the crime and mitigate any damage done. And finally, the

written program should include a detailed plan regarding how you will re-evaluate it on a periodic basis in order to account for changes in risk and technology. The FTC published a helpful booklet that offers businesses assistance in designing these programs. Also, low-risk businesses and organizations can take advantage of a program template that the FTC has put on its Red Flags Rule website—entities can fill out the relevant information directly online and print the document. See the section below on “Where Can I Find More Information?” for the links to the booklet and the template.

After implementation, the identity theft prevention program must be administered and managed on an ongoing basis by your organization’s board of directors or senior employees. It also must include appropriate staff training and provide for oversight of any service providers. The FTC does not conduct routine compliance audits, but it can conduct investigations to determine whether a business within its jurisdiction has complied with the Red Flags Rule. As a penalty for noncompliance, the FTC can seek both monetary civil penalties and injunctive relief. The law currently sets the maximum civil penalty at \$3,500 per violation. However, the FTC staff has advised that, as a matter of prosecutorial discretion, it would be unlikely to recommend bring an enforcement action against businesses under the following circumstances: (1) you know your clients individually, and therefore the likelihood of your business being defrauded by impersonation is very low; (2) you provide services to customers in or around their home, and therefore the risk of identity theft is extremely low because identity thieves do not want people to know where they live; or (3) identity theft is rare in your business, and therefore it is unlikely that identity thieves are targeting your sector.

WHEN must we comply?

The Red Flags Rule is already enforceable. It went into effect in January 2008 and became enforceable in August 2009.

WHERE Can I Find More Information?

There is a host of helpful information about the Red Flags Rule, including whether your organization will fall within the relevant definitions and how to design a compliant program. Everything can be found by going to the FTC’s website on the Red Flags Rule—www.ftc.gov/redflagsrule. Here are links to more specific sources within that website:

- The Red Flags Rule: www.ftc.gov/redflagsrule (or in pdf format at: <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>)
- An FTC-published booklet giving plain English compliance advice, “Fighting Fraud with the Red Flags Rule: A How-To Guide for Business”: <http://www.ftc.gov/redflagsrule>
- An FTC-made video on “Getting Ready for Red Flags”: <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/video.shtm>
- A template created by the FTC with step-by-step instructions on designing a program for businesses and organizations at low risk of identity theft: <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/diy-template.shtm>
- Frequently Asked Questions and their answers by the FTC staff: <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm>

- List of resources: <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/resources.shtm>
- For questions about compliance with the Red Flags Rule, you may also contact RedFlags@ftc.gov

This alert is meant to provide general information only and not legal advice. For further information, contact Lawyers Alliance for New York at (212) 219-1800 or visit our website at www.lawyersalliance.org for further information.

Lawyers Alliance for New York is the leading provider of business and transactional legal services for nonprofit organizations that are improving the quality of life in New York City neighborhoods. Our network of pro bono lawyers from law firms and corporations and staff of experienced attorneys work together, delivering expert corporate, tax, real estate, employment and other legal services to community organizations. By connecting lawyers, nonprofits and communities, we help nonprofits to develop affordable housing, stimulate economic development, and operate vital programs for children and young people, the elderly, recent immigrants, and other low-income New Yorkers.