



THE “RED FLAGS RULE”

Update Issued January 2010

On October 30, 2009, the Federal Trade Commission (“FTC”) announced that it is again extending the compliance deadline for the Red Flags Rule (“RFR”). The new deadline is June 1, 2010.

The extension comes at a time when the ultimate application of the RFR is unclear. For a discussion of the types of organizations that may be subject to the RFR, see our original Legal Alert below.

On October 29, 2009, members of Congress, including Health Finance Services Chairman Barney Frank (D-Mass.), urged the FTC to delay the RFR for at least 180 days. The House recently passed legislation which would exclude certain small businesses from the RFR and would also allow exemptions for organizations that demonstrate they either (1) know all their customers or clients individually; (2) only perform services in or around the residences of their clients; or (3) are engaged in a type of business in which identity theft is rare and the organization has not experienced incidents of identity theft. This legislation is now pending in the Senate.

On the same day, in a case brought by the American Bar Association, the District Court of the D.C. Circuit found that Congress had not intended the RFR to apply to law firms when it enacted the underlying legislation. The FTC had refused to grant attorneys an exemption from the RFR, arguing that law firms fall within the statute’s definition of “creditor” because they bill clients for services performed in the past. The Court rejected this argument. The decision may have implications for nonprofit organizations which could be deemed subject to the RFR because of similar billing practices. However, the impact of the Court’s ruling is yet to be seen.

If your organization instituted a written identity theft program in anticipation of the earlier November 1, 2009 enforcement deadline, it is probably desirable to continue following that program. For further guidance, please [contact](#) Senior Staff Attorney Leslie Kimball at our New York office.

Original Legal Alert Issued July 15, 2009

In January 2008, the “Red Flags Rule” (“RFR” or “Rule”), a regulation issued jointly by the Federal Trade Commission (FTC), the federal bank regulatory agencies and the National Credit Union Administration, came into effect. This rule requires certain organizations, which may include nonprofit organizations, to implement a written identity theft prevention program designed to detect the warning signs (“red flags”) of identity theft in their operations, to take steps to prevent the crime, and to mitigate the damages it inflicts. The initial deadline for complying with the RFR was November 1, 2008, but the deadline was extended to August 1, 2009 (and later extended again to November 1, 2009). Organizations to which the RFR applies that fail to develop the required procedures may be subject to civil monetary penalties.

In order to come under the RFR, two things need to be in place: 1) a determination that an organization is a Financial Institution or a Creditor; and 2) the organization offers or maintains Covered Accounts.

What is a “Creditor”?

A nonprofit may be considered a Creditor under the statute. Creditor is defined very broadly and includes businesses or organizations that regularly defer payments for goods and services and bill customers later.

A Creditor also includes:

- One who regularly grants loans, arranges for loans or the extension of credit, or makes credit decisions;
- Anyone who regularly participates in the decision to extend, renew, or continue credit, including setting the terms of credit; and
- A business that owns its own credit card, arranges credit for its customers, or extends credit by selling customers goods or services now and billing them later (simply accepting credit cards as a form of payment does not make a business a creditor under the Rule)

According to the FTC, the determination of whether an organization falls under the Rule is based on the organization's activities, not its particular area of business. If a nonprofit is engaging in activities that a for-profit would engage in or if a nonprofit collects payment information in order to bill for services rendered or goods provided, then a nonprofit is subject to the regulations. Although these regulations will primarily affect colleges, universities and hospitals, other nonprofit organizations may also be subject to the RFR.

What is a “Covered Account”?

If a nonprofit is a Creditor, it then must discern whether it holds a Covered Account, which the FTC defines as a “continuing relationship established by a person with a Financial Institution or Creditor to obtain a product or service for personal, family, household, or business purposes.” There are two types of Covered Accounts. The first type is basically a consumer account that involves multiple payments that are billed or payable monthly, including credit card accounts, mortgage loans, checking accounts, savings accounts, and more.

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.” Examples of this type of account include i) a nonprofit's records of personal information of its clients that its employees or the client may access remotely or ii) a single transaction consumer account that may be vulnerable to identity theft.

While the first type of Covered Account is always subject to the RFR, the second type of Covered Account is subject to the Rule only if the risk of identity theft is reasonably foreseeable. If you are unsure about whether you hold Covered Accounts, the FTC recommends considering how the accounts are accessed; remotely accessed accounts would be much more vulnerable to identity theft.

Examples of a nonprofit organizations that are covered by the RFR include: i) a social service organization that charges a fee for its services and allows installment payments; ii) a school lender under the Federal Family Education Loan Program; and iii) an organization that offers institutional loans to employees or others. If your organization determines that it is a Creditor that

does in fact have Covered Accounts, then it is a subject to the RFR and needs to create and implement an identity theft program.

Implementation of a Written Program to Identify and Detect Red Flags

Organizations covered by the RFR must implement a written program that identifies and detects the red flags of identity theft. The regulations do not specify any particular “technology, systems, process, or methodology,” that must be utilized, but the FTC says that the program must accomplish four things.

- First, the organization must identify red flags, which may include unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents;
- Second, it must put procedures in place to detect these red flags in everyday operations;
- Third, if red flags are detected, the organization must respond appropriately to mitigate identity theft; and
- Finally, the program must be updated often in order to respond to the frequently-changing nature of identify theft.

The specific nature of the program can vary based on a number of factors, including the size and scope of the organization, the type of business the nonprofit is engaged in, and the probability of identity theft. An organization is not required to educate its clients or customers about its identity theft safety measures.

The organization’s board of directors or a board committee must approve the written program and either the board or a senior employee may administer the program. Whoever is responsible for overseeing the program must also report annually either to the board of directors or to a designated senior manager. The report should discuss the program’s effectiveness, monitoring procedures, any incidents of identity theft, and any suggestions for changes to the program.

Sample Policies

The following websites contain sample red flag policies. Note that these are only samples prepared by other organizations and posted on the Internet, and should not be considered to be comprehensive policies applicable for every organization. Nonprofits subject to the RFR should construct their own policies to specially fit the characteristics of their organization. Please contact either Pro Bono Partnership or your attorney for help drafting your own policy.

<http://www.ama-assn.org/ama1/pub/upload/mm/368/red-flags-rule-policy.pdf>

http://www.nacubo.org/documents/business_topics/RedFlagSample1.pdf

<http://www.oml.org/cnt/files/websiteNews/10-%20Chickasha%20Red%20Flag%20Resolution.doc>

http://www.google.com/url?sa=t&source=web&ct=res&cd=13&url=http%3A%2F%2Fwww.acca-online.org%2Ffrontpage_articles%2FRedFlag%2FRed%2520Flag%2520Rules%2520Sample.doc&ei=pFhWSvyiEpCKNsG3uJ0I&rct=j&q=red+flags+rule+sample&usq=AFQjCNHjbku-ICTsTtKgPaHaRn8PI9q7UA

Additional Information

The FTC has published a How-To Guide in order to help organizations fulfill their duties under the Red Flags Rule. It can be found here:

<http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

The FTC also has put out a document detailing a “Do-It-Yourself Prevention Program” for complying with the RFR:

http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf

In addition, a number of federal agencies jointly put out a Frequently Asked Questions page regarding the Red Flags Rule, available at <http://www.ftc.gov/os/2009/06/090611redflagsfaq.pdf>

The original text of the Red Flags Rule, as found in the Federal Register, can be accessed at <http://www.occ.treas.gov/fr/fedregister/72fr63718.pdf>

IRS Circular 230 Disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of: (i) avoiding penalties under the Internal Revenue Code or any other U.S. federal tax law; or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein.

This document is provided as a general informational service to volunteers, clients, and friends of the Pro Bono Partnership. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does distribution of this document create an attorney-client relationship.

Copyright 2010 Pro Bono Partnership, Inc. All rights reserved. No further use, copyright, dissemination, distribution, or publication is permitted without the express written consent of Pro Bono Partnership, Inc.

January 2010