

## WSGR ALERT

MAY 2009

### FTC EXTENDS DELAYED ENFORCEMENT OF RED FLAGS RULE UNTIL AUGUST 1, 2009; PROVIDES GUIDED TEMPLATE TO ASSIST COMPANIES IN DEVELOPING IDENTITY THEFT PREVENTION PROGRAMS

On May 13, 2009, the Federal Trade Commission (FTC) released a template to help businesses comply with the Identity Theft Red Flags Rule (Red Flags Rule), a new rule that requires companies to adopt and implement an identity theft prevention policy.<sup>1</sup> The FTC has deferred enforcement of the rule until August 1, 2009.

This WSGR Alert gives a brief overview of the Red Flags Rule, its coverage, and its requirements.

#### Overview of Red Flags Rule

The Red Flags Rule, promulgated by the FTC and other regulators pursuant to Section 114 of the Fair and Accurate Credit Transactions Act (FACTA), requires creditors and financial institutions that maintain covered accounts to develop and implement written identity theft prevention programs. The identity theft prevention programs must be designed to help identify, detect, and respond to patterns, practices, and specific activities—known as “red flags”—that could indicate identity theft. Significantly, the program must be approved by the company’s board of directors (or, if the company lacks a board of directors, by an appropriate senior-level employee).

#### Applicability

As previously noted, the Red Flags Rule applies to all financial institutions and creditors that maintain covered accounts.

A “financial institution” includes any person or entity that holds a “consumer transaction account,” as defined in the Federal Reserve Act. Financial institutions that fall under the FTC’s jurisdiction include state-chartered credit unions, mutual funds that offer accounts with check-writing privileges, and other entities that offer accounts where a consumer can make payments or transfers to third parties. Most financial institutions are aware of their obligations under the Red Flags Rule.

Many entities that may be considered creditors, however, remain uncertain as to whether they are covered by the rule. A “creditor” is defined broadly to include “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 any original creditor who participates in the decision to extend, renew, or continue credit.”<sup>2</sup>

This definition covers all entities that regularly permit deferred payments for goods or services. As a result, many entities that do not consider themselves creditors may find themselves swept within the scope of the rule. For example, professionals, such as lawyers or healthcare providers, who bill clients after rendering their services, may be covered, as may retailers or service providers that regularly provide customers with products or services and then bill for those

products or services at the end of the month. The FTC has also stated that the definition includes “retailers that offer financing or help consumers get financing from others, say, by processing credit applications.” Companies should consider their business practices carefully to determine whether they are covered by the broad “creditor” definition.

Even if an entity is a financial institution or a creditor, the rule only obligates it to implement an identity theft prevention program if it maintains covered accounts. The rule defines a “covered account” as “(i) [a]n account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) [a]ny other account that the 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.”

#### Complying with the Rule

To comply with the Red Flags Rule, all creditors and financial institutions with covered accounts must develop and implement a program for combating identity

<sup>1</sup> The FTC’s guided four-step template is available at [http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags\\_forLowRiskBusinesses.pdf](http://www.ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf).

<sup>2</sup> FACTA incorporates the definition of “creditor” in the Equal Credit Opportunity Act (ECOA).

*Continued on page 2...*

## FTC Extends Delayed Enforcement of Red Flags Rule . . .

Continued from page 1...

theft in connection with those accounts. The program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft.

The rule employs a risk-based approach, by which the program should be appropriate to the size and complexity of the covered entity, as well as the nature of its operations. As a result, a large company with several types of covered accounts may need a complex program, while a small, low-risk business may be able to adopt a streamlined program.

In all cases, the program must include the following four elements:

- **Identification of red flags.** The covered entity should identify relevant patterns, practices, and specific forms of activity that are red flags signaling possible identity theft, and should incorporate those red flags into its program.
- **Detection of red flags.** The covered entity's program must be designed to detect the red flags it has identified.
- **Responses to red flags.** The program should spell out appropriate actions that the covered entity will take when it detects red flags.
- **Periodic review and updating.** The program should address how the covered entity will re-evaluate the program periodically and, as necessary, update the program to address new and evolving threats.

The program must be approved by the covered entity's board of directors (or a committee of the board) or, if the entity does

not have a board of directors, by an appropriate senior-level employee. The program must specify who is responsible for implementing and administering the program effectively.

The program also must include appropriate training for the covered entity's staff. Further, if the covered entity outsources or subcontracts any parts of its operations that would be covered by the Red Flags Rule, the entity's program must specify how it will monitor compliance with the program by the entity's subcontractors.

The FTC and the other agencies involved in the creation of the rule issued guidelines to assist financial institutions and creditors in developing and implementing their identity theft prevention program, including a supplement that provides several examples of red flags.<sup>3</sup> Additionally, the FTC published a simplified guide to assist businesses in understanding the scope of the rule and its requirements.<sup>4</sup>

Failure to comply with the rule may result in injunctive relief and civil penalties of up to \$2,500 for each knowing violation. The FTC has not commented on its enforcement of the rule, but it is likely that each covered account not protected in accordance with the rule would constitute a violation. This could result in very large civil fines. Additionally, failure to comply with the rule could result in claims under state consumer-protection laws.

### Implications

The FTC has cast a very wide net in defining the scope of entities subject to the Red Flags Rule. Many companies that do not typically view themselves as creditors, including nonprofit entities, doctors, attorneys, and

other professionals, will need to consider carefully whether they are covered.

Even in the absence of legal obligation, a program containing the elements required by the rule may help many companies mitigate the risk of identity theft and other unauthorized use of customers' sensitive personal information. The guidelines published by the FTC and other agencies, the FTC's guide for business, and the FTC's recently released template guide attempt to make complying with the Red Flags Rule less burdensome.

We anticipate that the ambiguity in the definition of "creditor," coupled with the general advisability of adopting an identity theft prevention program, will cause many entities that are uncertain of the rule's application to them to nonetheless adopt and implement an identity theft prevention program. Companies should also be aware that an identity theft prevention program, even for those covered by the rule, should be one component of a broader privacy and information security framework that employs safeguards appropriate to protect personally identifiable information held by the entity from unauthorized access, use, and disclosure.

Notably, in the news release accompanying the FTC's April 30, 2009, enforcement policy statement, FTC Chairman Jon Leibowitz acknowledged "the ongoing debate about whether Congress wrote [the portion of FACTA authorizing the FTC and other agencies to create and enforce the Red Flags Rule] too broadly," and stated that the FTC's most recent delay of enforcement "would allow industries and associations to share guidance with their members, provide low-risk entities an opportunity to use the template in

<sup>3</sup> The Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation (interagency guidelines) are published as Appendix A to 16 CFR Part 681. They are available at [www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf](http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf). The interagency guidelines are on pages 63,773 and 63,774 of that document.

<sup>4</sup> The FTC's guide for business, "Fighting Fraud with the Red Flags Rule," is available at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>.

Continued on page 3...

## **FTC Extends Delayed Enforcement of Red Flags Rule . . .**

*Continued from page 2...*

developing their programs, and give Congress time to consider the issue further.”

Congress may clarify whether retailers and some other businesses are subject to the Red Flags Rule, but in the interim, all businesses and organizations that fit the definitions of “creditor” or “financial institution” and maintain covered accounts should design and implement an appropriate identity theft management program.

Finally, although other jurisdictions maintain robust legal protections for consumer data,

the Red Flags Rule represents a significant, targeted effort by U.S. legislators and regulators to prevent and mitigate identity theft. Entities with international operations should be aware of the potential for other jurisdictions to adopt similar approaches.

Wilson Sonsini Goodrich & Rosati’s attorneys have experience helping clients comply with the FTC’s Red Flags Rule, as well as other marketing and privacy matters. If you have questions in these areas, please contact Lydia Parnes, Sara Harrington, or Matt Staples.



Wilson Sonsini Goodrich & Rosati  
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on May 18, 2009. To receive future WSGR Alerts and newsletters via email, please contact Marketing at [wsgr\\_resource@wsgr.com](mailto:wsgr_resource@wsgr.com) and ask to be added to our mailing list.

This communication is provided for your information only and is not intended to constitute professional advice as to any particular situation. We would be pleased to provide you with specific advice about particular situations, if desired. Do not hesitate to contact us.

650 Page Mill Road  
Palo Alto, CA 94304-1050  
Tel: (650) 493-9300 Fax: (650) 493-6811  
email: [wsgr\\_resource@wsgr.com](mailto:wsgr_resource@wsgr.com)

[www.wsgr.com](http://www.wsgr.com)

© 2009 Wilson Sonsini Goodrich & Rosati,  
Professional Corporation  
All rights reserved.