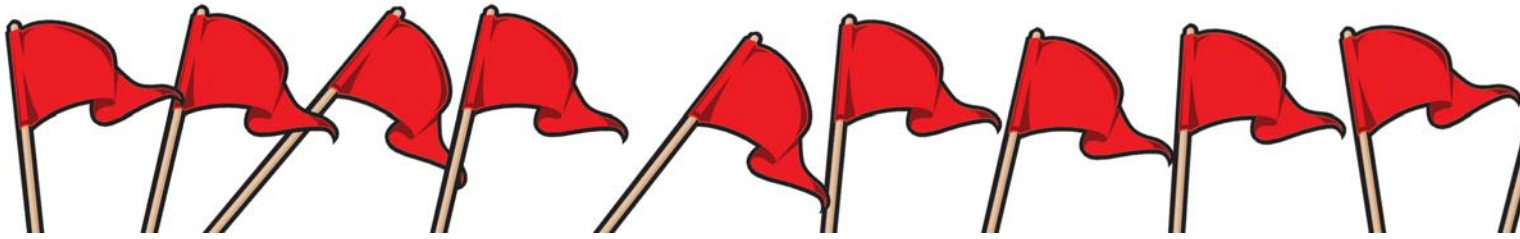

The "Red Flags" Rule: Are You New Requirements for Fighting

BY TIFFANY GEORGE AND PAVNEET SINGH

The expression "red flag" signals "Danger: Be alert to problems ahead." For millions of consumers every year, identity theft is more than a threat – it's their reality. The economic, psychological, and emotional harm to victims can be devastating. But businesses often bear the biggest part of the monetary damage from identity theft.

It's everyone's responsibility to do what they can to fight identity theft. But businesses and organizations that offer credit or other financial services can be the first to spot the red flags that signal the risk of identity theft, including suspicious activity indicating that identity thieves may be using stolen information like names, Social Security numbers, account numbers, and birth dates to open new accounts or raid existing ones.

Under the Red Flags Rule, which went into effect on January 1, 2008*, certain businesses and organizations are required to spot and heed the red flags that often can be the telltale signs of identity theft.

To comply with the new Red Flags Rule – enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) – you may need to develop a written "red flags program" to prevent, detect, and minimize the damage from identity theft.

Are you covered by the Red Flags Rule? If so, have you put into place the new procedures the Rule requires?

WHO MUST COMPLY?

Although every business or organization with an ongoing relationship with consumers should keep an eye out for the possibility of identity theft, the Red Flags Rule applies only to "financial institutions" and "creditors." To determine if your business or organization is covered by the Rule and required to develop a written identity theft Program, you'll need to answer two questions:

1. Is your business or organization either a "financial institution" or "creditor," as those terms are defined in the Rule?
2. If so, do you have "covered accounts"?

A "financial institution" is a bank, savings and loan, credit union, or other entity that holds a "transaction account" belonging to a consumer. A "transaction account" is an account that allows the owner to make payments or transfers. Examples include checking accounts, savings accounts that permit automatic transfers, and share draft accounts. Another example would be a brokerage account that allows consumers to write checks.

Your business or organization is a "creditor" if you regularly:

- extend, renew, or continue credit
- arrange for someone else to extend, renew, or continue credit
- are the assignee of a creditor who is involved in the decision to extend, renew, or continue credit

Under the Rule, "credit" means an arrangement by which you defer payment of debts or accept deferred payments for the purchase of property or services. In other words, payment is made after the

Complying with Identity Theft?

product was sold or the service was rendered. Some examples of creditors are finance companies, automobile dealers, mortgage brokers, utilities, and telecommunications companies. Even if you're a non-profit or government agency, you still may be a creditor if you accept deferred payments for goods or services. However, simply accepting credit cards as a form of payment does not make you a creditor under the Rule.

If you determine you're a financial institution or a creditor, the next step is to see if you have "covered accounts." There are two types of covered accounts. One is an account used mostly for personal, family, or household purposes that involves multiple payments or transactions. Examples include credit card accounts, mortgage loans, car loans, margin accounts, cell phone accounts, utility accounts, and checking or savings accounts.

The other is one for which there is a foreseeable risk of identity theft. For example, one type of account that should be considered for coverage because it may be vulnerable to identity theft is a small business or sole proprietorship account. In determining whether you have such an account, consider the risks associated with how the accounts may be opened or accessed – i.e. what type of interaction and documentation is required – as well as your experience with identity theft.

If your business or organization is a financial institution or creditor, but does not have any covered accounts, you don't need a program. But if you have covered accounts, you must develop a written program to identify and address the red flags that could indicate identity theft.

HOW TO COMPLY

The Rule doesn't tell you specifically what your red flags program must look like. Instead, it gives you flexibility to implement a program that best suits your business or organization, as long as it meets the Rule's requirements.

Your starting point for developing a program is the Guidelines issued with the Red Flags Rule, available at www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf. (The Guidelines are on pages 63,773-63,774 of the document.) The Guidelines list the issues you must consider in developing and maintaining a program appropriate for your business or organization. You also should draw on your own experience and knowledge about identity theft risks in developing your program.

There are four basic steps to designing a program to comply with the Rule:

1. Identify relevant red flags
2. Detect red flags
3. Prevent and mitigate identity theft
4. Update your program periodically

In addition, your program must spell out how it will be administered. The program should be appropriate to the size and complexity of your company or organization, as well as the nature of your operations.

IDENTIFY RELEVANT RED FLAGS

Under the Rule, financial institutions and creditors with covered accounts must develop a written program to identify the warning signs of identity theft.

The Guidelines describe the following categories of warning signs – red flags – that your

continued on page 20

***The "Red Flags" Rule**, continued from page 19*

program must identify and address:

- alerts, notifications, or warnings from a consumer reporting agency
- suspicious documents
- suspicious personally identifying information
- suspicious activity relating to a covered account
- notices from customers, victims of identity theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts

When identifying red flags, consider the nature of your business and the type of identity theft to which you might be vulnerable.

DETECT RED FLAGS

Once you've identified the red flags that are relevant to your organization or business, you must establish policies and procedures to detect them in your day-to-day operations.

For example, you may spot red flags when you verify a consumer's identity, authenticate customers, monitor transactions, or verify requests for changes of address. Some red flags may seem harmless on their own, but can signal identity theft when paired with other events, say, a change of address coupled with the use of an address associated with fraudulent accounts.

PREVENT AND MITIGATE IDENTITY THEFT

Your program must include appropriate responses to your red flags to prevent and mitigate identity theft. These responses could include monitoring an account, closing an account, not opening a new account, contacting the consumer when you spot a red flag, or a combination. Sometimes you may determine that no response is necessary. In other cases, certain events — such as a recent data breach, a phishing fraud that targeted your business or organization, or another suspicious activity — may raise the risk of identity theft and require specific preventive actions.

UPDATE YOUR PROGRAM PERIODICALLY

Because identity theft threats change, your program must describe how you will update it to ensure that you are considering new risks and trends.

ADMINISTERING YOUR PROGRAM

No matter how good your program looks on paper, the true test is how it works. Your program must describe how it will be administered, including how you will get the approval of your management, maintain the program, and keep it current.

According to the Rule, your program must be approved by your Board of Directors or, if your business or organization doesn't have a Board, by a senior employee. The Board or designated senior employee also must approve any material changes to the program. Your program should include staff training as appropriate, and provide a way for you to monitor the work of your service providers. The keys are to maintain oversight of the program, keep it relevant and current, and ensure that all necessary members of your staff — from the boardroom to the mail room — are on board. A program that stays in a filing cabinet isn't a good program.

PENALTIES FOR NONCOMPLIANCE

Although there are no criminal penalties for failing to comply with the Red Flags Rule, financial institutions or creditors that violate the Rule may be subject to civil monetary penalties. But there's an even more important reason for compliance: It's just plain good business. It assures your customers that you are doing your part to fight identity theft.

Have questions about how health care providers can comply with the Rule? E-mail RedFlags@ftc.gov.

* On October 22, 2008, the Federal Trade Commission issued an Enforcement Policy statement that delays enforcement of the Red Flags rule until May 1, 2009 (www.ftc.gov/opa/2008/10/redflags.shtm). Although the Rule is in effect, the FTC will wait until May 2009 to enforce it. This does not affect enforcement of the address discrepancy and credit card issuer rules. Nor does it affect compliance for entities not under the jurisdiction of the Commission. ■

Tiffany George and Pavneet Singh are attorneys in the Federal Trade Commission's Division of Privacy and Identity Protection.

***Editor's Note:** The "Red Flags" Rule goes into effect May 1, 2009, and FiSCA has developed a Member Guide, as well as a Model Red Flags Policies and Procedures Manual, which are intended to provide a general overview of the Red Flags Rule and an outline for an effective written identity theft prevention program. These, plus several customizable forms are all available to FiSCA members in the Compliance section at www.FiSCA.org*