Portfolio Media, Inc. | 648 Broadway, Suite 200 | New York, NY 10012 | www.law360.com
Phone: +1 212 537 6331 | Fax: +1 212 537 6371 | customerservice@portfoliomedia.com

The FTC Red Flags Rule — How It Works

Law360, New York (June 02, 2009) -- On Aug. 1, 2009, the Federal Trade Commission will begin enforcing its "Red Flags" Rule, 16 C.F.R. § 681.2, designed to help prevent and mitigate identity theft.

The rule does not address the need for data security measures, which help prevent identity thieves from obtaining unauthorized information. Instead, the purpose of the rule is to prevent identity thieves from using information they have illegally obtained.

Probably most of us think about identity theft as something that banks and credit card companies should watch out for, but the new regulations affect a wide range of businesses and services whose customers are individuals, sole proprietorships and small businesses.

The rule requires many businesses and organizations to create and implement written programs to identify and detect the warning signs of identity theft. Violation of the rule does not carry criminal penalties, but there are civil penalties for noncompliance of $3,500 per violation when the FTC brings an enforcement action.

FTC staff believe that over 11 million business entities are subject to the rule, which affects organizations, large and small, that regularly extend credit to businesses and individuals. Affected business entities include organizations that provide goods or services for which the customer pays after delivery, which means that many professional practices are affected.

If a business is subject to the Red Flags Rule, it must comply with the rule even if it is at low risk of encountering identity theft. In general, the more certain a business is that its customers are who they say they are, the lower the risk of encountering identity theft.

For example, most law firms with individual clients are probably low-risk businesses. Similarly, businesses that provide services at people's residences, such as gardening, cleaning and home repair are probably low-risk businesses.

For a low-risk business, the program can be relatively simple, focusing on how to respond to notifications or information suggesting that a customer's identity is being misused.

The FTC has created a template Red Flags Rule compliance program for low risk businesses, available at www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm.

The rule affects "creditors" with "covered accounts," as well as financial institutions. In deciding whether an organization must comply, it is important to consider how "creditor" is defined for purposes of the rule, because the term applies to many businesses, nonprofit groups and government agencies that are not typically thought of as "creditors."

The term "creditor" is broadly defined to include any entity that regularly extends, renews or continues credit. This means that a business (including a professional practice), a not-for-profit entity or a government entity that defers payment for goods or services may be considered a "creditor."

Creditors may include, among others, utility companies, vehicle dealers, retailers, educational institutions, medical service providers and telecommunications companies.

In an Enforcement Policy Statement, the FTC indicated that "any person that provides a product or service for which the consumer pays after delivery is a creditor."

In addition, a business is a "creditor" if it grants loans, arranges for loans or credit, or makes credit decisions. Accepting credit cards for payment (as opposed to issuing credit cards) does not in itself make an entity a "creditor."

There are two types of "covered accounts." The first is an account that is used primarily for personal, family or household purposes involving multiple payments or multiple transactions. The second is an account for which there is a foreseeable risk of identity theft, such as an account for a small business or sole proprietorship.

There are three major steps required for compliance.

First, if an organization is a "creditor" under the rule, it must determine whether it offers or maintains covered accounts. In making the determination, consider the methods used to open accounts, the methods used to access accounts, and previous experience with identity theft.

Second, if an organization offers or maintains covered accounts, it must establish a written program designed to detect and prevent identity theft and mitigate the effects of identity theft.

Written programs will vary, depending upon the nature of the business and the types of transactions and accounts it maintains. The board of directors, a committee of the board

or a designated senior management employee must be involved in developing the program.

A written program must include four elements:

1) Policies and procedures to identify the warnings (or “red flags”) of identity theft that may arise in the daily operations of a business.

Examples of red flags might include notifications from credit reporting companies, documents that appear altered, documents with information that is inconsistent with other information, an address or telephone number that has been used by many other people, an account that is used in a way that is different from the established pattern, information about unauthorized charges, and notices from law enforcement or a victim of identity theft.

2) Policies and procedures to detect the warnings that have been identified.

Examples of policies to detect red flags might include verifying customer identification when accounts are established, authenticating customers who access existing accounts, monitoring transactions, and verifying change-of-address requests. It may be appropriate to incorporate some of an organization’s existing practices, such as fraud detection practices, into the written plan.

3) Policies and procedures to respond to the warnings that have been detected. Examples of appropriate responses to red flags might include monitoring an account, contacting the customer, changing passwords or security codes and notifying law enforcement.

Covered entities may also determine that no response is necessary if, under the circumstances, there is a reasonable basis to conclude that a particular red flag does not indicate a risk of identity theft.

4) Policies and procedures to keep the program up to date, by evaluating it periodically and modifying it to reflect changing circumstances, such as changes to the business, changes in technology and changing tactics used by identity thieves.

Third, the organization must administer the written program. The initial written program must be approved by the board of directors or a committee of the board. In an organization that does not have a board of directors, a senior management employee must be designated to approve the program.

The board, or a board committee, or a senior management employee, must be involved in administration of the program. Staff must be trained to implement the program. And there must be oversight of service providers who open or manage accounts or bill customers or collect debts.

There are civil penalties for noncompliance of $3,500 per violation when the FTC brings an enforcement action. FTC staff says that the FTC is willing to resolve compliance issues informally if businesses make good-faith efforts to comply.

States are authorized to enforce the Red Flags Rule, too: they may seek injunctive relief, $1,000 for each willful or negligent violation, and attorneys' fees and costs. Under some circumstances, private plaintiffs may be able to sue for violations of the Red Flags Rule.

Further information is available in the Federal Trade Commission's Red Flags Rule how-to guide, "Fighting Fraud With The Red Flags Rule: A How-To Guide For Businesses," available at www.ftc.gov/redflagsrule.

--By Janine L. Scancarelli and Joel D. Smith, Folger Levin & Kahn LLP

Janine Scancarelli is a partner with Folger Levin & Kahn in the firm's San Francisco office. Joel Smith is an associate with the firm in the San Francisco office.

The opinions expressed are those of the authors and do not necessarily reflect the views of Portfolio Media, publisher of Law360.