



Business Law Information Memo

July 2009

Bond, Schoeneck & King, PLLC

New York

Albany ■ 518-533-3000
Buffalo ■ 716-566-2800
Ithaca ■ 607-330-4000
Long Island ■ 516-267-6300
New York City ■ 646-253-2300
Oswego ■ 315-343-9116
Rochester ■ 585-362-4700
Syracuse ■ 315-218-8000
Utica ■ 315-738-1223

Florida

Bonita Springs ■ 239-390-5000
Naples ■ 239-659-3800

Kansas

Overland Park ■ 913-234-4400

RED FLAG RULES PROGRAM MUST BE IN PLACE AUGUST 1ST

On August 1st, the twice-delayed Red Flag Rules take effect. The rules are required by the Fair and Accurate Credit Transactions Act of 2003. Every business that regularly extends credit must adopt and implement a written Identity Theft Prevention Program designed to detect the warning signs of identity theft, take steps to prevent it, and to mitigate the damage it inflicts. The theory behind the rules is that if red flags are identified in advance, organizations will be better equipped to spot suspicious patterns when they arise and better able to prevent a costly episode of identity theft.

Under the rules, “creditors” include organizations that regularly defer payment for goods or services, or provide goods or services and bill customers later. If a “creditor” maintains “covered accounts,” defined as consumer accounts that allow multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft, it must have a Red Flag program. Accounts opened and maintained for customers are generally considered “covered accounts” under the law. Billing customers later for goods or services delivered today is the extension of credit. Unless your business regularly gets cash on the barrel-head, it is a creditor covered by the Red Flag Rules.

ELEMENTS OF A RED FLAG PROGRAM

The Red Flag Rules are flexible. Each creditor must assess the risk of identity theft and develop a program based on those risks. The FTC has indentified four program components: identification of risks, detection, mitigation and responsibility.

Step One: Identify Relevant Red Flags

The FTC defines red flags as the “potential patterns, practices, or specific activities indicating the possibility of identity theft.” Companies must review their covered accounts for the possibilities of identify theft. The FTC has provided examples of red flags, including (1) notice from a customer, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently; (2) suspicious documents; (3) suspicious personal identifying information; (4) unusual use of a covered account; and (5) notices or warnings from consumer reporting agencies.

Specific red flags for businesses include:

- Fraud alert included on a customer’s credit report;
- A customer is unable to verify his or her identity when opening an account;
- Documents provided for identification appear forged or altered;

(continued)

BS&K publications are for clients and friends of the firm and are not a substitute for professional counseling or advice. For information about our firm, practice areas and attorneys, visit our interactive web site, www.bsk.com.

Attorney Advertising
© 2009 Bond, Schoeneck & King, PLLC
All Rights Reserved

Printed on recycled paper

BOND, SCHOENECK & KING, PLLC
ATTORNEYS AT LAW ■ NEW YORK FLORIDA KANSAS



- Information on the customer's identification inconsistent with what the customer is providing orally;
- Mail sent to the customer who has been extended credit is being returned as undeliverable.

Step Two: Detecting Red Flags

The second step is to identify how the company will detect each red flag that has been identified. For example, the company might consider reviewing proof of identity when opening an account or asking challenge questions with respect to the information contained on the identifying documents. It might also limit access to account information internally to a need-to-know basis.

Step Three: Mitigating Impact

The third step requires planning a response to red flags. Remember, this does not mean that there has been an actual identity theft, only that a red flag, an indication of possible identity theft, has been detected. Appropriate responses might include working with staff on responding to the specific incident, reviewing whether further staff training is necessary, and reviewing whether procedures need to be changed.

The facts of a particular case will oftentimes warrant a combination of appropriate responses, or require a different response altogether. Sometimes, notice to a consumer or law enforcement may be necessary; other times, no action may be necessary. Perhaps a new account number should be issued. The program must include a plan for response.

Step Four: Responsibility for the Program

The Red Flag program must be approved by the organization's board of directors or an appropriate committee designated by the board. The board or the committee should oversee, develop, implement and administer the program, or it may designate a "senior employee" to do the job. If a "senior employee" is designated, the employee's name must be listed in the program. For organizations that do not have a board of directors, the FTC has stated that "a designated employee at the level of senior management" shall act in that capacity.

The program must also list the categories of employees who will be trained to detect red flags, and how they will be trained. There should be a brief annual training and an orientation for new employees as well. The program must be periodically updated and assessed to ensure that the organization is keeping current with identity theft risks.

The program must also describe how the organization plans to supervise service providers who may detect red flags that have been identified. For example, if the organization hires a collection agency to collect overdue bills, the organization must require the collection agency to follow the organization's program or have a program of its own to follow.

Although there is great flexibility in designing a Red Flag program, every business that extends credit must put a program in place. Companies cannot determine that they have zero risk and need no program.

In Buffalo / Niagara Falls, call 716-566-2800 or e-mail:
Robert A. Doren rdoren@bsk.com

In the Capital District, call 518-533-3000 or e-mail:
Hermes Fernandez hfernandez@bsk.com

In Central New York, call 315-218-8000 or e-mail:
Edwin J. Kelley, Jr. ekelley@bsk.com

In Garden City, call 516-267-6300 or e-mail:
Terry O'Neil toneil@bsk.com

In the Mohawk Valley, call 315-793-2723 or e-mail:
Linda E. Romano lromano@bsk.com

In New York City, call 646-253-8000 or e-mail:
Louis P. DiLorenzo ldilorenzo@bsk.com

In Northern New York, call 315-343-9116 or e-mail:
John D. Allen jdallen@bsk.com

In the Rochester Region, call 585-362-4700 or e-mail:
Robert H. Kirchner rkirchner@bsk.com