

“RED FLAGS” IDENTITY THEFT RULES

The Federal Trade Commission (FTC) has issued a set of regulations, known as the “Red Flags Rule,” requiring that certain entities develop and implement written identity theft prevention and detection programs to protect consumers from identity theft. The enforcement date of the Red Flags Rule is November 1, 2009.

WHAT IS THE PURPOSE OF THE RED FLAGS RULE? According to the FTC, as many as 9 million Americans have their identities stolen each year. The Red Flags Rule was developed by the FTC to require “creditors” and “financial institutions” to develop and implement policies and procedures to prevent and detect such theft. Identity theft occurs when someone uses another’s personal identifying information (e.g., name, Social Security number, credit card number, or insurance enrollment or coverage data) to commit fraud or other crimes.

DOES THE RULE APPLY TO MY BUSINESS? While you may not think of yourself as a “creditor” (you most likely are not a “financial institution”), the term as defined in the Rule is quite broad. NKBA Members may fall into the category of “creditors” if they offer customers the ability to pay for goods and services after receipt of such goods or services. Any business that receives payment after services are provided, even if it’s collected in full after final delivery and installation, is considered a “creditor” under the law. Likewise, you may fall into the “creditor” category because you arrange for customers to obtain credit to pay for services through a financing company. On the other hand, requiring payment before or at the time of contracting, or simply accepting credit cards as a form of payment at the time of service, does not make the company a creditor under the Rule. In short, the only way to avoid qualifying as a creditor under the Rule seems to be to **always** require payment at the time the service is provided.

If your business is considered to be a “creditor” under the Rule, you must then determine if you have “covered accounts”. A “covered account” is defined as:

- (a) all consumer accounts that permit multiple payments or transactions, and
- (b) any other account which poses a reasonably foreseeable risk to a consumer or business from identity theft.

Thus, you should consider any account that contains personal identifying information that could allow someone to steal a client’s identity as a “covered account.” Your customer records may meet this definition because they include the owner’s name and address and may contain payment information (such as credit card numbers, etc.). If the customer pays by personal check and you have a copy of their driver’s license in the file, it is a covered account.

OK, MY BUSINESS IS A CREDITOR WITH COVERED ACCOUNTS. WHAT DOES THE LAW REQUIRE? If your business comes within the definition of “creditor” and you have “covered accounts”, then you must put into place reasonable policies and procedures designed to detect the warning signs –or “red flags” – of identity theft in your day-to-day operations, and take steps to prevent the crime and limit the amount of damage it causes.

A “Red Flag” is defined as a suspicious pattern, practice or specific activity that indicates the possibility of identity theft. The FTC has identified the following as Red Flags:

- (a) alerts, notifications or warnings from a credit reporting agency;
- (b) suspicious documents and/or personal identifying information, such as a suspicious address change;
- (c) unusual use of, or suspicious activity relating to, a covered account; and
- (d) notices of possible identity theft from customers, victims of identity theft or law enforcement authorities regarding possible identity theft.

As an example, if a customer has to provide some form of identification to open an account with your company, information on the ID that is not consistent with the information provided by the customer might be a red flag that something is amiss. Likewise, if an ID that is presented looks like it might be fake, that too would be a red flag for your business.

WHAT MUST THE IDENTITY THEFT PREVENTION PROGRAM INCLUDE?

The Program must contain “reasonable policies and procedures” to:

- (a) identify relevant Red Flags for covered accounts;
- (b) detect when the selected Red Flags are triggered;
- (c) describe the appropriate response when a Red Flag is detected to prevent and mitigate against loss; and
- (d) establish procedures to periodically update your Program to allow for revisions as technology and circumstances change.

Step One: Identify Relevant Red Flags. First, you should review the list of the Red Flags issued by the FTC in Supplement A to the Rule, available at ftc.gov/redflagrule and identify those that are relevant to your business. In addition, as you review your files you may identify other Red Flags not on the list but still relevant to your business. A full copy of the Rule is available at:

<http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>

Step Two: Detecting and Addressing Red Flags. Once you have identified and documented the Red Flags relevant to your business, you need to develop

and document the procedures you and your staff will take to address those Red Flags if they are encountered.

These procedures may include actions such as:

- (a) contacting the customer to verify or report the information;
- (b) requesting additional identifying information;
- (c) monitoring the account for suspicious activity;
- (d) refusing to provide services to that customer, or refusing to hire the applicant;
- (e) notifying the appropriate authorities; or
- (f) concluding that no action is necessary at that time.

Step Three: Formalizing and Administering the Red Flags Program.

Approval of the Program. The initial Program must be approved by your Board of Directors or appropriate committee of the Board; if your business does not have a Board of Directors, then someone in senior management must approve the plan.

Responsibility for administering the Program. Either the Board or a senior employee must oversee, develop, implement and administer the Program. Responsibilities include assigning specific responsibility for the Program's implementation, reviewing staff reports about how your business is complying with the Rule, and approving modifications to the Program.

Training the staff. You are required to train relevant staff in identity theft deterrence and detection. The training program should provide the following information:

- (a) the purpose of the program;
- (b) identification of Red Flags your business may encounter;
- (c) the proper procedures for reporting and responding to Red Flags.

All staff should receive a copy of the actual written Program, and should sign a form that acknowledges and documents that they have read it and received the training. Copies of these signed forms should be kept in an administrative file.

Monitoring of Service Providers. In addition, you are required to monitor the conduct of your service providers if they are conducting activities covered by the Rule, such as billing customers, providing customer service, or collecting debts to ensure that they are applying the same standards of identity theft prevention as you are. According to the FTC, you can comply with this requirement by including in your contracts that such companies have procedures in place to detect Red Flags and either report triggering events to you or respond appropriately to prevent and mitigate the crime themselves.

Periodic Review and Evaluation. You must periodically review and evaluate your business's written Identity Theft Prevention Program as required by the Rule. The Program should be reviewed and modified as needed at least annually and more frequently if needed.

IS THERE A SAMPLE THEFT IDENTITY PROGRAM THAT I CAN USE FOR MY BUSINESS? Yes. The FTC has created a number of booklets and pamphlets that you can use to assist you in complying with the Red Flags Rule. One such booklet, [Fighting Fraud with the Red Flags Rule: A How-To Guide for Businesses](#), is a clear, simple guide to complying with the law. In addition, there is a six-page, fill-in-the-blank form with step-by-step instructions on designing a Program for businesses which are at low risk for identity theft: [Do-It-Yourself Prevention Program for Business and Organizations at Low Risk for Identity Theft](#).

WHAT HAPPENS IF I DON'T HAVE MY PLAN IN PLACE BY THE NOVEMBER 1ST DEADLINE? The FTC most likely will not be checking-up on businesses to see if they have their Identity Theft Protection Program in place on the 1st. Enforcement of the Rule against every business in the country which may be impacted will be impossible. But that doesn't mean that you should ignore the Rule if it applies to your business. If an identity theft occurs in your company, the FTC may very well investigate the incident and evaluate your compliance with the law. If you are found to be in violation of the Rule, it will be too late to develop and implement a Program and you will likely be subject to civil liability and governmental sanctions, and possibly state and federal criminal liability suits as well. Currently, the federal law sets \$3,500 as the maximum civil penalty per violation.

ADDITIONAL SOURCES CONCERNING IDENTITY THEFT PREVENTION ARE AVAILABLE FROM THE FTC TO ASSIST YOU FURTHER

- [Fighting Back Against Identity Theft](#)
- [Identity Theft, Privacy, & Security](#)
- [Protecting Personal Information: A Guide for Business](#)
- [Information Compromise and the Risk of Identity Theft: Guidance for Your Business](#)
- [Teach Your Colleagues \(resources to educate your employees and clients\)](#)
- [Using FTC Resources for Education Partnership](#)