Franchisors: Are You Complying with the Red Flags Rule’s New Requirements for Fighting Identity Thef

As many as nine million Americans have their identities stolen each year. The economic, psychological, and emotional harm to victimized consumers can be devastating. The cost to businesses — left with unpaid bills racked up by scam artists — can be staggering too.

The Red Flags Rule, a law the FTC will begin to enforce on August 1, 2009, requires certain businesses — including some franchisors — to develop a written program to spot the warning signs — or “red flags” — of identity theft. Is your franchise system covered by the Red Flags Rule? If so, have you developed your Identity Theft Prevention Program to detect, prevent, and minimize the damage that could result from identity theft?

WHO MUST COMPLY

Every franchise system must review its billing and payment procedures to determine if it’s covered by the Red Flags Rule. Whether the law applies to you isn’t based on your status as a franchisor, but rather on whether your activities fall within the law’s definition of two key terms: “creditor” and “covered account.”

Franchisors may be covered by the Rule if they are “creditors.” Although you may not think of your business as a “creditor” in the traditional sense of a bank or mortgage company, the law defines “creditor” to include any entity that regularly defers payment for goods or services or arranges for the extension of credit. Franchisors are creditors if they makes loans to prospective franchisees or arrange third-party lenders for a prospective franchisee. Further, franchisors are creditors if they bill their franchisees after providing services. However, simply accepting credit cards as a form of payment does not make a franchisor a creditor under the Rule.

The second key term — “covered account” — is defined as a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft. The collection of payments from franchisees in connection with the operation of a franchised business ordinarily is not for a personal, family, or household purpose and, therefore, would not qualify as this type of “covered account.” Accordingly, a franchisor generally would fall under

the Red Flags Rule only if it determines that there is a reasonably foreseeable risk of identity theft in its business. For example, an account with a foreseeable risk of identity theft may include a small business or sole proprietorship account that is closely linked to the personal information of an individual officer or owner. Depending upon the particular facts, a franchisee may be a small business for this purpose.

If your franchise system is a creditor, but does not have any covered accounts, you don’t need a program. But if your franchise system is a “creditor” with “covered accounts,” you must develop a written Identity Theft Prevention Program to identify and address the red flags that could indicate identity theft in those accounts.

SPOTTING RED FLAGS

The Red Flags Rule gives covered franchisors flexibility to implement a program that bests suits the operation of their system, as long as it conforms to the Rule’s requirements. Your system may already have a fraud prevention or security program in place that you can use as a starting point.

If you’re covered by the Rule, your program must:

- Identify the kinds of red flags that are relevant to your business;
- Explain your process for detecting them;
- Describe how you’ll respond to red flags to prevent and mitigate identity theft; and
- Spell out how you’ll keep your program current.

What red flags signal identity theft? There’s no standard checklist. Supplement A to the Red Flags Rule — available at ftc.gov/redflagsrule — sets out some examples, but here are a few warning signs that may be relevant to franchisors:

- Suspicious documents. Has a prospective franchisee given you identification documents that look altered or forged? Is the photograph or physical description on the ID inconsistent with what the prospective franchisee looks like? Did the prospective franchisee give you other documentation inconsistent with what he or she has told you — for example, an inconsistent date of birth or address mentioned elsewhere? Under the Red Flags Rule, you may need to ask for additional information from that prospect.
- Suspicious personally identifying information. If a prospective franchisee gives you information that doesn’t match what you’ve learned from other sources,

it may be a red flag of identity theft. For example, if the prospect gives you a home address, birth date, or history of business experience that doesn’t match what you have on file for that prospect — such as information submitted to a lead generator or what the prospect told you in an initial request for information — fraud could be afoot.

- Suspicious activities. You may spot red flags of identity theft in the process of reviewing applications and negotiating contracts. Is mail returned repeatedly as undeliverable, even though the prospect still communicates with you? Does your email to a prospect bounce back or does the prospect ignore faxes? Questionable activities may be red flags of identity theft.

- Notices from victims of identity theft, law enforcement authorities, insurers, or others suggesting possible identity theft. Have you received word about identity theft from another source? Cooperation is key. Heed warnings from others that identity theft may be ongoing.

SETTING UP YOUR IDENTITY THEFT PREVENTION PROGRAM

Once you’ve identified the red flags that are relevant to your practice, your program should include the procedures you’ve put in place to detect them in your day-to-day operations. Your program also should describe how you plan to prevent and mitigate identity theft. How will you respond when you spot the red flags of identity theft? For example, if a prospective franchisee provides a photo ID that appears to be forged or altered, will you request additional documentation? If you’re notified that an identity thief has requested financing using another person’s information, how will you ensure that the debt is not charged to the victim? Finally, your program must consider how you’ll keep it current to address new risks and trends.

No matter how good your program looks on paper, the true test is how it works. According to the Red Flags Rule, your program must be approved by your Board of Directors or, if your business doesn’t have a Board, by a senior employee. The Board or senior employee may oversee the administration of the program, including approving any important changes, or designate a senior employee to take on these duties. Your program should include information about training your staff and provide a way for you to monitor the work of your service providers — for example, those who manage your system’s collection operations. The key is to make sure that all members of your staff are familiar with the Rule and your new compliance procedures.

WHAT’S AT STAKE

Although there are no criminal penalties for failing to comply with the Rule, violators may be subject to financial penalties. But even more important, compliance with the Red Flags Rule assures the public that you’re doing your part to fight identity theft.

Looking for more information about the Red Flags Rule? The FTC has published Fighting Fraud with the Red Flags Rule: A How-To Guide for Business,
a plain-language handbook on developing an Identity Theft Prevention Program. For a free copy of the Guide and for more information about compliance, visit ftc.gov/redflagsrule.
In addition, the FTC has released a fill-in-the-blank form for businesses and organizations at low risk for identity theft. The online form offers step-by-step instructions for creating your own written Identity Theft Prevention Program. You can fill it out online and print it. The do-it-yourself form is available at ftc.gov/redflagsrule.

Questions about the Rule? Email RedFlags@ftc.gov.

Steven Toporoff is an attorney with the FTC’s Division of Privacy & Identity Protection.