



Raising A Red Flag

Insights

10.29.09

Many schools have been contacted by vendors advising that the school must set up an identity theft program to comply with the new federal regulations called the "Red Flags Rule." This rule was implemented by the Federal Trade Commission (FTC) and mandates that financial institutions and creditors with covered accounts develop and implement a written program that detects, prevents, and mitigates identity theft.

If your school operates like most private schools (as discussed below), you will likely find that your tuition payment practices will place the school squarely within the definition of a "creditor with covered accounts," thus requiring implementation of an Identity Theft Program. This article discusses the purpose of the Red Flags Rule, the definitions, and guidelines for both removing your school from coverage or coming into compliance.

The purpose of the Red Flags Rule is to protect consumers from identity theft. The Rule essentially requires covered entities to have policies and processes in place to combat identity theft. If entities do not have a program that complies with the Red Flags Rule, they could risk being subject to fines or civil litigation.

Is Your School Considered A "Creditor" Under The Rule?

The Red Flags Rule applies to creditors. The term "creditor" is defined broadly under the Rule. In fact, the FTC's Business Alert explained that "[a] creditor is any entity that regularly extends, renews, or continues credit . . .," *which includes those not for profit entities that "defer payment for goods or services . . ."* In plain English, a creditor regularly provides goods or services and accepts payment for those goods or services *after* they have been delivered.

In the context of private and independent schools, if you provide education to a student without demanding (and ensuring) that the tuition is paid up front before the service is rendered, you are a creditor. In addition, if you permit parents to pay for tuition on a payment plan, and ask them to sign an enrollment contract for the coming school year, setting forth a set number of payments over the course of the year, you are also considered a creditor under the Rule. On the other hand, if you require payment upfront or "pay as you go" – so that students could be barred from class if they don't pay – you will not be considered a creditor under the Rule.

But the regulations do make clear that to constitute a creditor, an entity has to be "regularly" engaged in the extension of credit. Consequently, a one-time deferral of payment would not

constitute being regularly engaged in the extension of credit.

Does Your School Maintain "Covered Accounts"?

Additionally, the Red Flags Rule applies only to creditors who maintain a "covered account." Essentially, a covered account is any account maintained by a creditor primarily for personal, family, or household purposes, and involves or is designed to permit multiple payments or transactions. Schooling is definitely a personal and familial service. And, if schools accept the payment of tuition by way of multiple transactions, the particular account for which they accept such payment would be considered a covered account under the Red Flags Rule.

Accordingly, depending on the nature of a school's tuition payment plan, it is possible that schools may be considered creditors with covered accounts. Therefore, at the very least, schools should consult with their legal counsel to determine the applicability of the Red Flags Rule to their institution. And even if the manner in which schools currently carry out their tuition plan does not bring them under the ambit of the Red Flags Rule, they should regularly monitor their tuition plans to determine whether any new or existing accounts are being carried out in a way that might cause them to fall under the Red Flags Rule.

What Measures Must Be Taken To Comply?

If you are a creditor and maintain covered accounts, the Red Flags Rule requires the creation and implementation of a written program which sets forth policies and procedures that effectively detect, prevent, and mitigate identity theft in connection with the opening of new or existing covered accounts. While the Rule initially required compliance by November 2008, the FTC has delayed enforcement until November 1, 2009.

The Rule is flexible with respect to the scope of an entity's identity theft prevention program, understanding that it will vary depending on the extent of a creditor's activity which would implicate identity theft issues.

Generally speaking, an identity theft program must include the following:

Identify and detect the red flags that are relevant to your institution

You can identify red flags applicable to your institution by reviewing the 26 Red Flag indicators published by the FTC and determining which indicators are applicable to your covered accounts.

Respond to and report red flags

Ultimately schools have to determine who is going to be responsible for the administration and oversight of the Identity Theft Program. All reports of potential identity theft issues should be directed to the administrator of the program. The administrator is then responsible for responding to such reports. Appropriate responses may vary depending on the nature of the report but could include: monitoring the account, contacting the customer, closing the account, or notifying law enforcement.

Ensure that the program is periodically updated

Mark your calendar for yearly updates to your school's Identity Theft Program. In addition, you should review the program when an identity theft problem arises by looking at any changes that need to be made in the program to detect prevent, and mitigate identity theft, or any changes that should be made to the covered accounts.

The rule also makes clear that it is not enough to simply have a written identity theft program. In addition:

- the Identity Theft Program must be approved in writing by the board of directors or a committee of the board, and such approval must be maintained with the policy;
- relevant staff (those staff members that come into contact with covered accounts) must be trained on the program;
- there must be appropriate oversight of the program; and
- a board or person must be appointed as the program administrator who is responsible for overseeing and continually reviewing the Identity Theft Program.

The FTC webpage sets forth the FTC's Do-It-Yourself Prevention Program for Low Risk Businesses, the completion and application of which would put low risk businesses in compliance with the Red Flags Rule. To view the Program [click here](#).

It's important that all schools undertake an appropriate analysis of the way they transact their business to determine the applicability of those regulations.