

RED FLAGS RULE

What Schools Need To Know To Be Compliant

Red Flags Rule Summary Information

Definitions Pertinent to the Red Flags Rule

How the Rule Applies to Colleges and Universities

Will You Need to Implement A Policy?

Steps To Be Taken By Colleges/Universities Covered by the Rule

Additional Resources

Red Flags Rule Checklist

Red Flags Rule Summary Information

- The Red Flags Rule (Rule) is part of the Fair and Accurate Credit Transaction (FACT) Act of 2003. After four extensions, enforcement of the Rule begins **December 31, 2010**.
- The overall intent of the Rule is to mitigate instances of identity theft.
- The Rule requires creditors to develop and implement programs that provide for the identification, detection, and response to “red flags” that could indicate identity theft.
- “Creditor” as defined by the Rule and the Federal Trade Commission (FTC) includes colleges and universities that award Perkins Loans and/or offer deferred payment plans (including third-party payment plans).
- Recipients of information from national credit reporting agencies (for background checks, hiring, or any other reason) must also have a policy in place.
- The college or university’s board of directors (or appropriate board committee) must approve the initial written program, if the college or university is identified as a creditor. Board approval may be necessary only for the first written program if the board delegates to appropriate senior management further responsibility.
- The program should be reviewed and updated annually.
- While the FTC does not typically have jurisdiction over not-for-profit entities, it has indicated that it will be the Rule enforcement agency for colleges and universities.

Consequences for Noncompliance

Failure to comply with the Red Flags Rule may result in FTC-assessed fines of up to \$1,500 per consumer file. In addition to the potential fines, an institution could compromise its reputation with alumnae, students, and prospective students, resulting in significant additional financial losses.

Definitions Pertinent to the Red Flags Rule

The following definitions help explain how the Rule must be applied:

- **Red Flag:** A pattern, practice, or specific activity that indicates the possible existence of identity theft. This may include (but is not limited to) suspicious behavior, presenting identification which may have been altered or fake, and unfamiliarity with information related to the account or account holder.
- **Financial Institution:** Any entity holding a consumer transaction account, including banks (state, national, or mutual savings), savings and loan associations (federal or state), and credit unions (federal or state).
- **Creditor:** Any entity that offers deferred payment options or that bills customers after providing goods or services. In addition, creditors are entities that make loans, extend credit, and process credit applications for credit to be offered by a third party, or are involved in renewing, extending, or continuing existing credit.
- **Account:** A continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, household, or business purposes.
- **Covered Account:** Two types of covered account are defined by the FACT Act: a consumer account and a foreseeable risk account. Consumer accounts are those primarily tied to individuals or households, such as credit cards, utilities, etc., which may allow balances to be paid over time. Foreseeable risk accounts are those where the creditor or financial institution may not be able to protect the consumer information it collects and stores. A consideration of how accounts are accessed should be included in a determination of whether certain accounts are “covered” (i.e. may the account be accessed remotely/electronically), as this may increase the potential for identity theft. A covered account may be an existing account or a newly created account.

How the Rule Applies to Colleges & Universities

- A periodic risk assessment should be conducted to determine if covered accounts exist at the institution. This should be done as part of an annual review of policies and procedures and related documentation.
- Colleges and universities offering students an ID that also operates as a Visa or MasterCard debit card should coordinate with the bank through which such services are offered to ensure that the bank has an adequate identity theft prevention program in

place. Confirmation of the bank’s program (e.g., a copy of the bank’s program, a letter from the bank confirming that it has such a program, etc.) should be included in the college or university’s documentation for the Rule.

- The FTC has taken a risk-based approach to this new rule. This approach requires the institution to determine if it acts as a creditor, assess the level of identity theft risk associated with any covered accounts, and, implement a policy which mitigates that risk. This approach allows flexibility in the scope of any program implemented by the institution.

Will You Need to Implement A Policy?

The following questions will help to determine if your institution must implement a policy to adhere to the Rule:

<p>1. Is the institution a <u>creditor</u>?</p> <p>Yes or No</p>	<p>If yes, continue to question #2.</p>
	<p>If no, the institution may not need to comply with the Red Flags Rule; however the process of making this determination and the conclusions reached should be documented.</p>
<p>2. Are any of the institution’s accounts <u>covered accounts</u>?</p> <p>Yes or No</p>	<p>If yes, then a written compliance program must be developed. <u>Go to “Steps to be taken...”</u></p>
	<p>Since the institution has already identified itself as a creditor (by responding “yes” to question #1 above), it is likely that some (if not all) of its accounts are covered accounts. A “no” determination at this point should be double-checked and heavily documented. If “no” is the final determination, then a program is not required for compliance. A regularly scheduled review of institutional practices should be undertaken to ensure that the institution remains in compliance (i.e. because of changes in business practices the institution may eventually become a creditor or financial institution and have covered accounts as defined above).</p>

Steps to be Taken by Colleges/Universities Covered by the Rule

Under the Rule, creditors that hold covered accounts must develop an identity theft prevention program that includes reasonable policies and procedures to detect or mitigate identity theft and enable the creditor to:

1. **Identify** relevant "red flags" (i.e., patterns, practices, and specific activities that signal possible identity theft) and incorporate them into the program;
2. **Detect** the red flags that the program incorporates;
3. **Respond** appropriately to detected red flags to prevent and mitigate identity theft; and
4. **Update** the program periodically to reflect changes in risks.

The board of directors (or an appropriate committee) must approve the initial written program. Board approval may be necessary only for the first written program if the board delegates to appropriate senior management further responsibility. **If an institution has not yet done so, it should promptly develop an identity theft prevention program for board or committee approval, as the Red Flags Rule went into effect November 1, 2008, and enforcement begins on December 31, 2010.** The [checklist](#) included at the end of this document will assist in the creation of a compliant program.

Identification

The institution must determine its red flags within the definition provided by the FACT Act of 2003. Some examples include:

- Altered or falsified identification;
- Description information on identification does not match photo or presenter of the ID
- Duplicate Social Security Number;
- Address or phone number occurring repeatedly for multiple customers (students, parents, staff, etc.);
- Person making contact is unable to confirm other account information/accurately respond to challenge questions;
- Account activity continues to occur, however there is information showing that the account holder is not receiving invoices (returned mail, contact from account holder saying no invoice received, etc).

Detection

In addition to identifying what should be considered a red flag, institutions must also have a process to detect when red flags have occurred.

The detection efforts may include:

- Training staff how to recognize, record, and report suspected red flag activity they encounter.
- Ensuring that all requested information to establish an account has been provided and matches other available information (e.g., Institutional Student Information Record (ISIR) information matches the application for admission, the billing address, etc.).
- Scheduling regular reports generated by the student information system (SIS) that:
 - o Compare student addresses or phone numbers & search for duplications;
 - o Track recent changes of address or banking information and when student refund is issued;
 - o Identify how changes were made to information (i.e., phone, online, in person, etc). NOTE: Changes made online have a higher likelihood of being fraudulent.
- Establishing an individual or group of individuals who act as the point of contact for all red flag-related activity by monitoring and reporting the activity.
 - o The use of a single person, email distribution list to a team, and/or the ability of staff to easily record suspected red flag activity on the SIS (with frequent reporting of this information) are key to maintaining the vigilance required by the Rule. Collection of data without a central repository or analysis could lead to multiple red flags on an account going unnoticed and noncompliance.

Response

Once red flags have been identified and detected, the institution must respond to the situation according to an established plan, and notify the affected parties. Responses and communication should correlate to the potential risk associated with the identified red flags. The institution's plan may identify different levels of risk with unique corresponding responses.

Some responses included in the FACT Act include:

- Contact the customer;
- Restrict access to the account by changing passwords, security codes, and limiting other means of accessing or changing account information;
- Close existing account;
- Open a new account with verified customer information as outlined in the Customer Identification Program Rules (31 CFR 103.121);
- Do not send the account to a collection agency; and
- Notify law enforcement.

Update

The program of identification, detection and response should be reviewed and updated on a scheduled or as-needed basis to ensure that changes to business practices have not created new vulnerabilities and that compliance remains a staff responsibility. Changes such as new campus ID cards, software systems, staff turnover, and other examples may compromise a previously adequate program.

Additional Resources

Red Flags Rule as published in the Federal Register:

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

Federal Trade Commission publication (PDF): “Fighting Fraud with the Red Flags Rule, a How-To Guide for Business” <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

Federal Trade Commission Red Flags Rule website:

<http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml>

Delay of Enforcement to December 31, 2010 Announcement:

<http://www.ftc.gov/opa/2010/05/redflags.shtm>

Department of Education (ED) DCL “Update on FTC ‘Red Flags Rule’ that Applies to Institutions Participating in the Perkins Program” (via NASFAA):

<http://www.nasfaa.org/publications/2009/earedflags052209.html>

Red Flags Rule Checklist

Each task should be completed on or before December 31, 2010, the beginning date of enforcement.

- Develop initial written identity theft prevention plan including how the institution will:
 - Identify what constitutes a red flag
 - Detect when red flags occur
 - Respond to the occurrence

- Determine which office(s) and individuals are responsible for implementing and maintaining the plan (including regular review & updates).

- Develop training program for identified offices and individuals, including subsequent new employees.

- Submit identity theft prevention plan to board of directors or a committee for review and approval.

- Obtain board (or committee) approval for plan, including authorization for appropriate senior management to continue development of the plan.

- Identify where the written policy is to be kept and communicate this information to all affected staff and/or faculty.