




# Rensselaer

VICE PRESIDENT FOR FINANCE AND  
CHIEF FINANCIAL OFFICER

## MEMORANDUM

July 16, 2009

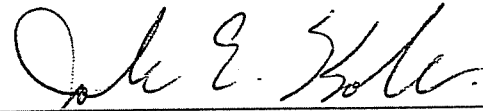
TO: John Kolb  
Charles Carletta

FROM: Virginia Gregg 

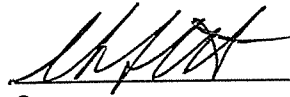
RE: Red Flags Rule Policy

The President has asked that you both concur with the enclosed policy prior to her final approval. John, it is my understanding that your staff was involved in its development, which I appreciate. As the regulation becomes effective August 1, your earliest attention would be appreciated. In my absence next week, if you have questions, please direct them to Sue Proskine.

Thanks.



Concurrence  
John Kolb  
Vice President for Information Services and  
Technology & Chief Information Officer



Concurrence  
Charles Carletta  
Secretary of the Institute & General Counsel

Enclosure




# Rensselaer

VICE PRESIDENT FOR FINANCE AND  
CHIEF FINANCIAL OFFICER

## MEMORANDUM

July 13, 2009

TO: Shirley Ann Jackson, Ph.D.  
President

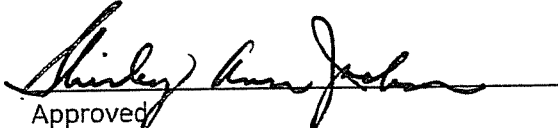
FROM: Virginia C Gregg   
Vice President for Finance & Chief Financial Officer

RE: Red Flags Rule Policy

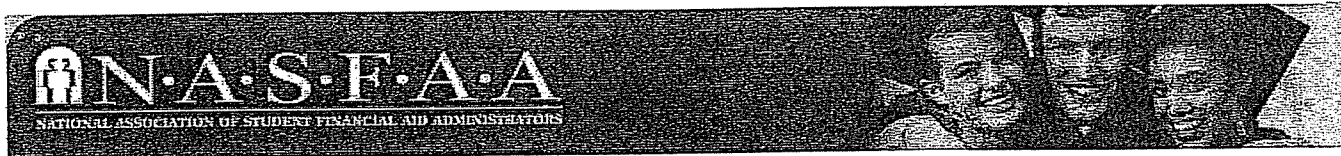
As outlined in the attached news bulletin from the National Association of Student Financial Aid Administrators, the Federal Trade Commission is requiring creditors and financial institutions to develop and implement written identity theft prevention programs. The U.S. Department of Education has opined that these rules apply to colleges and universities that participate in the Federal Perkins Loan Program, and may apply if an institution participates as a school lender under FFELP, offers institutional loans and/or offers an extended tuition payment plan. Rensselaer participates/offers all of these programs.

The regulation becomes effective August 1, 2009. The attached policy outlines Rensselaer's compliance with the regulation. Please note your approval of the policy below, or let me know if you require further clarification.

Thank you.

  
Approved

Enclosures



Home    Encyclopedia    Standards of Excellence    Reauthorization    LearnStudentAid.org    Parents & Students

[Print/Save Friendly Version](#)

**NASFAA WEB CENTERS**

- [NEWS](#)
- [NATIONAL CONVERSATION INITIATIVE](#)
- [MEMBERSHIP](#)
- [LEGISLATIVE](#)
- [REGULATORY](#)
- [RESEARCH](#)
- [TRAINING](#)
- [CONFERENCES](#)
- [TECHNOLOGY](#)
- [COLLEGE ACCESS](#)
- [NASFAA CATALOG](#)
- [CAREER CENTER](#)
- [EVENTS CALENDAR](#)
- [MEDIA](#)

**NEWS FROM NASFAA**

**FTC Provides Additional Three-Month Forbearance on 'Red Flag Rule' Enforcement**

The Federal Trade Commission announced it will delay enforcement of the new "Red Flags Rule" another three months -- until August 1, 2009 -- to give creditors and financial institutions more time to develop and implement written identity theft prevention programs.

The FTC also said it would soon release a template to help entities that have a low risk of identity theft, such as businesses that know their customers personally, comply with the law.

On Oct. 14, 2008, the Department of Education announced that the "Red Flags Rules" apply to institutions participating in the Federal Perkins Loan Program and may apply to other credit programs administered by an institution. The rule states that "creditors" holding "covered accounts" must comply with the law. The rules have a broad definition of "creditors" and "covered accounts" that is applicable to many colleges.

This is the second time that the FTC has delayed enforcement of the regulations that require financial institutions and creditors to develop and implement a written identity theft prevention program to detect, prevent, and respond to patterns, practices, or specific activities that may indicate identity theft. The regulations were included in the Fair and Accurate Credit Transactions Act (FACT Act) and institutions were expected to be in compliance by Nov. 1, 2008, but the FTC suspended enforcement until May 1, 2009. The initial six-month delay was designed to give creditors and financial institutions additional time to develop and implement written identity theft prevention programs.

"Given the ongoing debate about whether Congress wrote this provision too broadly, delaying enforcement of the Red Flags Rule will allow industries and associations to share guidance with their members, provide low-risk entities an opportunity to use the template in developing their programs, and give Congress time to consider the issue further," FTC Chairman Jon Leibowitz said.

Naomi Lefkowitz, an attorney in the FTC's Division of Privacy and Identity Protection, said that institutions will generally be subject to "Red Flag" requirements if they loaning out money and collecting it. If an institution is a "creditor" it must then determine if it is holding "covered accounts" - a consumer account that involves multiple payments or transactions (a loan that is billed or payable monthly).

Under this definition, the following activities could make institutions a "creditor" with "covered accounts:"

- participating in the Federal Perkins Loan program,
- participating as a school lender in the FFELP,
- offering institutional loans to students, faculty, or staff, or
- offering an extended tuition payment plan throughout the semester instead of requiring full payment at the beginning of the semester.

**Red Flags Rules Resources**

- [FTC Rule's requirements alert](#)
- [FTC Red Flags Rules Web site](#)

search

**NASFAA**  
 1101 Connecticut Avenue, NW,  
 Suite 1100  
 Washington, DC 20036-4303

Phone: 202-785-0453  
 Fax: 202-785-1487  
 Web@NASFAA.org

- [EDUCAUSE Red Flags Online Resource Center](#)
- [National Association of College and University Business Officers \(NACUBO\) Red Flags guidance](#)

By [Haley Chitty](#)  
NASFAA Director of Communications

*Posted 05/05/09 to [www.NASFAA.org](http://www.NASFAA.org). Redistribution to non-NASFAA institutions is prohibited. Please submit Web Site questions or comments to [Web@NASFAA.org](mailto:Web@NASFAA.org).*

[Home](#) | [Encyclopedia](#) | [Standards of Excellence](#) | [Reauthorization](#) | [LearnStudentAid.org](#) | [Parents & Students](#)

Copyright 2009 National Association of Student Financial Aid Administrators (NASFAA)

# RENSSELAER POLYTECHNIC INSTITUTE

## RED FLAGS RULE POLICY

### **Purpose**

The purpose of this policy is to establish a Red Flags Rule Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission’s Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003. Sections 114 and 115 of FACTA require higher education institutions to enact certain policies and procedures by August 1, 2009. This Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

- Identify relevant Red Flags for covered accounts the University offers or maintains and incorporate those Red Flags into its Program;
- Detect Red Flags that have been incorporated into the Program of the University;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft;
- Ensure the Program is updated periodically to reflect changes in risks to students and borrowers and to the safety and soundness of the University from identity theft; and
- The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

### **Existing Policies and Practices**

The University has policies to ensure compliance with Gramm-Leach-Bliley (GLB) and Family Educational Rights and Privacy Act (FERPA), as well as system and application security, and internal control procedures which provide an environment where identity theft opportunities are mitigated. Records are safeguarded to ensure the privacy and confidentiality of student and borrower records.

In addition, the University adheres to the following practices:

- All paper files are kept in locked filing cabinets while not being used.
- Access to confidential information is limited to only those employees who need access in order to properly perform the duties for which they were hired.
- Employees with access to confidential information understand that this is confidential business information and is not to be discussed with anyone who does not “need to know.”

## Definitions

- **Identify theft** means fraud committed or attempted using the identifying information of another person without authority.
- **Account** means a continuing relationship established by a person with the creditor to obtain a product or service for personal purposes. Account includes an extension of credit involving a deferred payment.
- **Covered account** means an account that a creditor offers or maintains primarily for personal purposes that involves or is designed to permit multiple payments or transactions.
- **Red Flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

## Covered Accounts

- The University participates in the Federal Perkins Loan Program and other Institutional Loan Programs
- The University offers and establishes student payment plans

## Identifying Relevant Red Flags

- The photograph or physical description on the identification is not consistent with the appearance of the student or borrower presenting the identification.
- The SSN provided is the same as that submitted by other students or borrowers.
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other students or borrowers.
- The person opening the covered account or the student or borrower fails to provide all required personal identifying information on an application or in response to notification that the application is complete.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account – nonpayment when there is no history of late or missed payments.
- The University is notified of unauthorized charges or transactions in connection with a student or borrower's covered account.
- The University is notified by a student or borrower, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

## **Detecting Red Flag Activity**

Covered accounts are opened as follows:

### **Federal Perkins Loan Program and Institutional Loan Programs**

- Perkins borrowers sign their promissory notes using an electronic signature, which requires a PIN number that is unique to each borrower.
- Perkins borrowers can allow a third party to have access to his/her account information by completing the FERPA form in the electronic exit interview process. If no one is listed, a third party will not have access to any account information without the borrower's written permission. The borrower can log onto the exit site at any time to update this information if he/she decides that it would be beneficial for another party to have access to account information.

### **Student Payment Plans**

Students must call, e-mail or come into the Bursar's Office to request their account be placed on a tuition payment plan.

### **Responding to Red Flags**

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

- Contacting the student or borrower;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Closing an existing covered account;
- Not attempting to collect on a covered account;
- Notifying law enforcement; and/or
- Determining that no response is warranted under the particular circumstances.

## **Updating the Program**

The University will update the Program as needed, to reflect changes in risks to students or borrowers or to the safety and soundness of the University from identity theft, based on factors such as:

- The experiences of the University with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft; and
- Changes in the types of accounts that the University offers or maintains.

## **Oversight of Service Provider Arrangements**

The University shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the University engages a service provider to perform an activity in connection with one or more covered accounts.

Currently the University uses UAS to administer the Perkins Loan Program and other Institutional Loan Programs. Students contact UAS directly through its website or by telephone and provide personal identifying information to be matched to the records that the University has provided to UAS.