

Rollins College Policy

Identity Theft Prevention Program

Red Flag Rules

The Federal Trade Commission has issued a final rule (the Red Flag Rule) under the Fair and Accurate Credit Transactions Act of 2003. The Red Flag Rule requires institutions that hold “covered accounts” (accounts for which a person makes repeat payments, see section II B) to develop and implement an identity theft prevention program for new and existing accounts.

Rollins College takes the possibility of identity theft seriously and in full compliance with the Red Flag Rule, has developed and implemented an Identity Theft Program (Program). After consideration of the size of the College’s operations and account systems, and the nature and scope of the College’s activities, the Board of Trustees determined that this Program was appropriate for Rollins College, and therefore approved this Program.

I Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program under the Red Flag Rules 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 guidelines and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to Students and to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

II Definitions

A) Identify theft means fraud committed or attempted using the identifying information of another person without authority.

B) Covered account means:

1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is

designed to permit multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts; and

2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to students or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

C) **Red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

III Identification of Relevant Red Flags

The Program shall include relevant red flags from the following categories as appropriate:

- A) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- B) The presentation of suspicious documents, such as appearing altered or forged;
- C) The presentation of suspicious personal identifying information, such as a photograph or physical description on the identification that is not consistent with the appearance of the student presenting the identification;
- D) A request made from a non-College issued E-mail account;
- E) A request to mail something to an address not listed on file;
- F) The unusual use of, or other suspicious activity related to, a covered account; and
- G) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

IV Detection of Red Flags

The Program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- A) Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
- B) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

V Response

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:

- A) Monitor a covered account for evidence of identity theft;

- B) Deny access to the covered account until other information is available to eliminate the red flag, or close the existing covered account;
- C) Contact the student;
- D) Change any passwords, security codes or other security devices that permit access to a covered account;
- E) Reopen a covered account with a new account number;
- F) Notify law enforcement; or
- G) Determine no response is warranted under the particular circumstances.

VI Updating the Program

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

- A) The experiences of the organization with identity theft;
- B) Changes in methods of identity theft;
- C) Changes in methods to detect, prevent and mitigate identity theft;
- D) Changes in the types of accounts that the organization offers or maintains;
- E) Changes in the College's business arrangements with other entities.

VII Oversight of the Program

The Vice President of Finance and Treasurer is responsible for the Program and oversight of the Program shall include:

- A) Assignment of specific responsibility for implementation of the Program and ensuring appropriate training of College's staff in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected;
- B) Reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft;
- C) Determining which steps of prevention and mitigation should be taken in particular circumstances;
- D) Review of reports prepared by staff regarding compliance; and
- E) Approval of material changes to the Program as necessary to address changing risks of identity theft.

Reports shall be prepared as follows:

- A) Staff responsible for development, implementation and administration of the Program shall report to the Vice President of Finance and Treasurer at least annually on compliance by the organization with the Program.
- B) The report shall address material matters related to the Program and evaluate issues such as:
 - 1) The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
 - 2) Service provider agreements;
 - 3) Significant incidents involving identity theft and management's response; and

- 4) Recommendations for material changes to the Program.

VIII Oversight of Service Provider Arrangements

The College 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 organization engages a service provider to perform an activity in connection with one or more covered accounts.

Currently the College uses Campus Partners to administer Perkins Loan repayments. Students contact Campus Partners directly through its website or by telephone and provide personally identifying information to be matched to the records that the College has provided to Campus Partners.

The College also uses a third-party vendor, Tuition Management Systems, to administer our installment payment plan for tuition payments.

IX Duties Regarding Address Discrepancies

Rollins College shall develop guidelines and procedures designed to enable the College to form a reasonable belief that a credit/consumer agency request relates to the consumer for whom it was requested. If the College receives a notice of address discrepancy from a consumer reporting agency indicating the address given by the consumer/student differs from the address contained in the consumer report, the College may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the consumer/student;
2. Review of the College's records;
3. Verification of the address through third-party sources; or
4. Other reasonable means.

If an accurate address is confirmed, the College shall furnish the student's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The College establishes a continuing relationship with the consumer/student; and
2. The College, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

X Penalties and FTC Enforcement

Although there are no active plans to audit organizations, a negative event could trigger an investigation of the institution. Any negative event such as a data breach, or even a

whistle blower, could open the institution up to monetary penalties and civil litigation. There are three areas of concern when discussing penalties:

- **Federal Trade Commission.** The FTC is authorized to bring enforcement actions in federal court for violations, and could enact penalties of up to \$2500 for each violation of the rule.
- **State Enforcement.** States are authorized to bring actions on behalf of their residents and may recover up to \$1000 for each violation, and may recover attorney's fees.
- **Civil Liability.** This is where organizations stand to lose the most. Not only will the organization suffer damage to its reputation and subsequent customer churn, but each consumer may be entitled to recover actual damages sustained from a violation. There is the possibility of class action law suits potentially resulting in massive damages.

APPROVED BY THE AUDIT COMMITTEE OF THE BOARD OR TRUSTEES:

March 25, 2009