RIBGHE

RHODE ISLAND BOARD OF GOVERNORS FOR HIGHER EDUCATION

IDENTITY THEFT RED FLAGS PROGRAM

I. PURPOSE

The Rhode Island Board of Governors for Higher Education adopts this Program to conform with the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 and to help protect the University of Rhode Island, Rhode Island College and the Community College of Rhode Island (herein collectively the "institutions") and their employees, students, and contractors from damages related to the loss or misuse of personal indentifying information contained in certain financial accounts maintained by or on behalf of the institutions.

This Program is intended to help the institutions:

1. Identify risks that signify potentially fraudulent activity within new or existing accounts subject to the law.

2. Detect risks when they occur in such accounts;

3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and

4. Update the Program periodically, including reviewing the accounts that are covered and the identified risks that are part of the Program.

II. COVERED ACCOUNTS

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing financial account or loan (including accounts covered by the Federal Perkins Loan Program) of students, employees, contractors, consultants, temporary workers, and other workers at the institutions that involve or are designed to permit multiple payments or transactions and for which there is a reasonably foreseeable risk of identity theft is covered by this Program. Whenever a Red Flag appears in connection with a covered account it shall be investigated to determine if any fraud or identity theft has been attempted or committed.

III. IDENTIFICATION OF RED FLAGS

A Red Flag is "a pattern, practice, or specific activity that indicates the possible existence of identity theft." In order to identify relevant Red Flags, the institution should consider the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The following Red Flags in each of the listed categories are potential indicators

of fraud; however, this list is not all inclusive and is subject to revision due to operational and technical developments:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity, such as
    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;

2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

3. Other document with information that is not consistent with existing information that is on file with the institution; and

4. Application for service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the student or employee provides (example: inconsistent birth dates);

2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);

3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5. Social security number presented that is the same as one given by another student or employee, has not been issued, or is listed on the Social Security Administration's Death Master File;

6. An address or phone number presented that is the same as that of another person;

7. A person fails to provide complete personal identifying information on an application when reminded to do so; and

8. A person's identifying information is not consistent with the information that is on file for the student or employee.

9. When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the student's name;

2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student or employee is repeatedly returned as undeliverable;
5. Notice to the institution that a student or employee is not receiving mail sent by the Institution;

6. Notice to the institution that an account has unauthorized activity;
7. Breach in the institution's computer system security; and
8. Unauthorized access to or use of student account information.

E. Alerts from Others

Red Flag

1. Notice to the institution from a student, Identity theft victim, law enforcement or other person that the institution has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, institution personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and

2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing covered account, institution personnel will take the following steps to monitor transactions on an account:

Detect

1. Verify the identification of students or employees if they request information (in person, via telephone, via facsimile, via email);

2. Verify the validity of requests to change billing addresses by mail or email and provide the student or employee a reasonable means of promptly reporting incorrect billing address changes; and

3. Verify changes in banking information given for billing and payment purposes.

C. Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, or in the event that the institution requires a credit report in connection with a covered account, institution personnel will take reasonable steps to assist in identifying address discrepancies. These steps may include:

1. Determining if the address in the credit report matches the address in its records; and

2. Verifying the institution's records; and

3. Requiring written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and

4. Using other reasonable means including but not limited to obtaining information from third party sources; and

5. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report

was made and report to the consumer reporting agency an address for the applicant that the institution has reasonably confirmed is accurate; and

V. RESPONDING TO RED FLAGS

In the event that potentially fraudulent activity is detected the employee discovering the same shall promptly alert the institution's Controller who shall review all relevant information and attempt to ascertain whether the attempted transaction was fraudulent or legitimate.

Should institution personnel detect any identified Red Flags, such personnel under the direction of the institution's Controller, shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor a covered account for evidence of identity theft;
2. Contact the student or applicant (for which a credit report was run);
3. Change any passwords or other security devices that permit access to covered accounts;
4. Not open a new covered account;
5. Provide the student with a new student identification number;
5. Notify law enforcement;
6. File or assist in filing a written report documenting the suspicious activity. Said report shall be submitted to the institution's Controller.

7. Determine, after consultation with the institution's Controller, that no response is warranted under the particular circumstances.

Protect Student Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the institution will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;

2. Ensure complete and secure destruction of paper documents and computer files containing student account information, pursuant to approved institution records retention schedules and the requirements of Rhode Island Law, when a decision has been made to no longer maintain such information;

6. Ensure that office computers with access to covered account information are password protected;

7. Avoid use of social security numbers, except where necessary to meet state or federal legal requirements;

8. Ensure computer virus protection is up to date; and

9. Require and keep only the kinds of student information that are necessary for the institution's purposes.

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the institution's Vice President for Administration (URI), Vice President of Administration and Finance (RIC) and Vice President of Business Affairs (CCRI) (hereinafter collectively "Vice President") who shall work in consultation with the Associate Commissioner of Higher Education – Finance and Management. The institution's Vice President will be responsible for ensuring appropriate training of institution staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Periodic Review

At least annually, the institution's Controller shall review these protocols and Program and recommend any changes to the institution's Vice President who shall review these recommendations with the Associate Commissioner for Higher Education – Finance and Management. The institution's Vice President shall at least annually, by December 31st, report to the Board of Governors' Facilities/Finance and Management Committee on the status of the institution's compliance with the Fair and Accurate Credit Transactions Act's identity theft requirements. This report should address material matters related to the Program and evaluate issues such as: the effectiveness of the institution's 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; service provider arrangements; significant incidents involving identity theft and the institution's response; and recommendations for material changes to the Program. The Facilities/Finance and Management Committee, upon its review of these reports, shall forward them to the Board of Governors for its acceptance thereof.

C. Staff Training and Reports

Staff training shall be conducted for all employees who may have access to covered accounts and the personally identifiable information contained therein. The training shall be supervised by the institution's Controller in consultation with its Director of Human Resources. Records of training agenda and attendees will be retained in accordance with approved institution records retention schedules.

All employees who may have access to covered accounts and the personally identifiable information contained therein shall be specifically directed to this Program.

D. Oversight of Vendors and Service Provider Arrangements

In the event the institution engages an outside vendor or service provider to perform an activity in connection with one or more covered accounts, the institution will take the following steps to ensure the service provider performs

its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

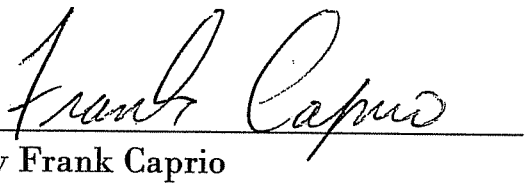
1. Require, by contract, that outside vendors and service providers have such policies and procedures in place; and

2. Require, by contract, that outside vendors and service providers review the institution's Program and report any Red Flags to the Controller or the institution employee with primary oversight of the vendor or service provider relationship.

VII. EFFECTIVE DATE

This Program shall be effective as of May 1, 2009.

Rhode Island Board of Governors
For Higher Education



By Frank Caprio
Chairman