Procedure 3.6:	Red Flags Rule (Identity Theft Prevention)
Volume 3:	Office of Business & Finance
Managing Office:	Office of Business & Finance
Effective Date:	December 2, 2014

I. Purpose

In 2007, the Federal Trade Commission (FTC) and Federal banking regulatory agencies issued a regulation known as the "Red Flags Rule" intended to reduce the rism0 0 1 72.024 535.51 Tm[(I)13(n)-9duce the ri

Category Two: Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or not authentic.
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 identifying information that is not consistent with existing student or employee information.
4. Application for service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Category Three: 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 provided by student or employee (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.
6. An address or telephone 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 notified to do so.
8. A person's identifying information is not consistent with the information that is on file for the student.

Category Four: Suspicious Activity or Unusual Use of Covered 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 is repeatedly returned as undeliverable.
5. Notice to the University that a student is not receiving mail sent by the University.
6. Notice to the University that an account has unauthorized activity.
7. Breach in the University's computer system security.
8. Unauthorized access to or use of student account information.

Category Five: Alerts from Others

Red Flags

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

b. Detecting Red Flags

Student Enrollment

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

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).

Existing Accounts

In order to detect any of the red flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, and via email).
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes.
3. Verify changes in banking information given for billing and payment purposes.

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, University personnel will take the following steps to assist in identifying address discrepancies:

1. Require 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.
2. 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 University has reasonably confirmed is accurate.