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 risk of identity theft. Under these rules, institutions that provide credit must develop and implement written identity theft prevention programs that provide for the identification, detection and response to patterns, practices or specific activities known as "Red Flags" that could indicate identity theft. The Red Flags Rule defines "creditors" and "covered accounts" very broadly. Parts of the rule or activities that may impact the University, as well as other colleges and universities include:

- Participating in the Federal Perkins Loan program;
- Participating as a school lender in the Federal Family Education Loan Program;
- Offering institutional loans to students, faculty, or staff, or
- Offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

This policy governs the methods and procedures that Alabama A&M University will execute to ensure compliance with the Federal Trade Commission's "Red Flags Rule," which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

II. Definition

a. Identity Theft - a fraud committed or attempted using the identifying information of another person without authority.

b. Red Flag -a pattern, practice, or specific activity that indicates the possible existence of identity theft.

c. Covered Account- all student and employee accounts or loans that are administered by the University.

d. Program Administrator- the individual designated with primary responsibility for oversight of the program.

e. Identifying information - any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

I. Authority, Responsibility, and Duties

a. Under the Federal Trade Commission's "Red Flags Rule," the University is required to establish an "Identity Theft "Prevention Program" tailored to its size, complexity and the nature of its operation.
b. The University shall establish an Identity Theft Committee to develop the Procedures regarding the Program's administration.
c. The University shall identify relevant red flags for new and existing covered accounts and incorporate those red flags into the Program.
d. The University shall categorize the severity of red flags using the following categories: Low Risk Red Flags, Medium Risk Red Flags, and High Risk Red Flags.
e. To prevent and mitigate identity theft, the University shall respond appropriately to any red flags that are detected, regardless of the category.
f. Each area responsible for monitoring identity theft must be deemed proficient by the appropriate University designee.
g. Each area responsible for monitoring identity theft must provide reporting to Senior Management.
h. The University shall ensure the Program is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the student and employee from identity theft.

III. Policy Statements

a. Identification of Red Flags

In order to identify relevant red flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. The University identifies the following red flags in each of the five listed categories:

Category One: Alerts, Notifications and/or 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 history and usual pattern of activity.

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.

c. Preventing and Mitigating Red Flags

In the event University personnel detect any identified red flags, such personnel 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) when a red flag is detected.
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.
6. Notify the Program Administrator for determination of the appropriate step(s) to take.
7. Notify the University Police Department.
8. Notify the University Internal Audit Department.
9. File or assist in filing a Suspicious Activities Report ("SAR").
10. Determine 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 University 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 when a decision has been made to no longer maintain such information.
3. Ensure that office computers with access to Covered Account information are password protected.
4. Avoid use of social security numbers.
5. Ensure computer virus protection is up-to-date.
6. Require and keep only the kinds of student information that are necessary for official University purposes.

References

www.nacubo.org/x10848.xml
www.ftc.gov/bcp/edu/pubs/business/alerts/alt05.shtm