Florida Agricultural & Mechanical University
Board of Trustees Policy

Board of Trustees Policy Number: 2009-01	Date of Adoption: May 4, 2009 Date of Revision: June 6, 2013

Subject	**Identity Theft Prevention Policy**
Authority	**16 CFR Part 681, Federal Trade Commission, Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transaction Act of 2003**
Applicability	**To establish guidelines to identify activity commonly associated with identity theft ("RED FLAGS") and to prevent and mitigate identity theft for the benefit of the students and employees of Florida A&M University.**

I. POLICY STATEMENT AND PURPOSE

The Florida Agricultural and Mechanical University Board of Trustees (FAMU or University) establishes the Policy and Procedures to provide the manner by which employees in critical departments of the University can identify activities commonly associated with identity theft and mitigate and prevent theft for the benefit of the students and employees of FAMU.

II. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program

1. *Identity Theft* - A fraud committed or attempted with the unauthorized use of identifying information of another person.

2. *Red Flag* - A pattern, practice, or specific activity that indicates the possible existence or attempt of identity theft.

3. *Covered Account* – Account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. A covered account is also an account for which there is a foreseeable risk of identity theft.

4. *Program Administrator* – University Chief Financial Officer.

5. *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.

B. Fulfilling Requirements of the 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. Each program must contain reasonable policies and procedures to:

1. Identify relevant "Red Flags" for new and existing covered accounts 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.

4. Ensure the Program is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the students and employees fromidentity theft.

III. IDENTIFICATION OF RED FLAGS

To identify relevant Red Flags, FAMU 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. FAMU identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

<u>Red Flags</u>

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.

5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

Red Flags

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

2. Identification document on which a person's photograph or physical description is inconsistent with the person presenting the document.

3. Other document with information that is not consistent with existing student or employee information.

4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the person provides (e.g., inconsistent birth dates).

2. Identify information presented that is inconsistent with other sources of information (e.g., an address not matching an address on a loan application).

3. Identify 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 (e.g., an invalid phone number or fictitious billing address).

5. Social security number presented that is the same as one given by another person.

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.

8. A person's identifying information is inconsistent with the information that is on file for the person.

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 person's name.

2. Payments stop on an otherwise consistently up-to-date account.

3. Account used in a way that is inconsistent with prior use.

4. Mail sent to the person is repeatedly returned as undeliverable.

5. Notice to the University that a person 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 person's account information.

E. Alerts from Others

Red Flag

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

IV. DETECTING RED FLAG

A. 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:

Detect

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

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, University personnel will take the following steps to monitor transactions on an account:

Detect

1. Verify the identification of students 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 a reasonable means of promptly reporting incorrect billing address changes.

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

C. Consumer ("Credit") Report Requests

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:

Detect

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.

V. PREVENTING AND MITIGATING IDENTITY THEFT

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 person (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 person with a new identification number.

6. Notify the Program Administrator for determination of the appropriate step(s) to take.

7. Notify law enforcement.

8. File or assist in filing a Suspicious Activities Report ("SAR").

9. Determine that no response is warranted under the particular circumstances.

Protect Student Identifying Information

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 unless required by law.

5. Ensure computer virus protection is up to date.

6. Require and keep only the kinds of student information that are necessary for University purposes.

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an

Identity Theft Committee ("Committee") for the University. The Committee is headed by a Program Administrator who may be the President or the President's designee. Two or more other individuals appointed by the President, the President's designee or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of FAMU 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. Staff Training and Reports

University staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University staff shall be trained to effectively implement the Program. Initial training shall be completed within one month of being involved with a covered account and annually thereafter, within two months of the end of each fiscal year. The Program Administrator shall also require training as deemed necessary. Signed records of attendees shall be kept by the Program Administrator. University employees are expected to immediately notify the Program Administrator once they become aware of an incident of identity theft or of the University's failure to comply with this Program. By December 15 of each year and as otherwise requested by the Program Administrator, University staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

C. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University 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 service providers have such policies and procedures in place.

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

D. Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students or employees and the soundness of the University from identity theft. In doing so, the Committee will consider the University's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.