FAYETTEVILLE STATE UNIVERSITY

IDENTITY THEFT PREVENTION
(RED FLAGS RULE)

Authority: Issued by the Fayetteville State University Board of Trustees.

Category: University-Wide

Applies to: ●Administrators ●Faculty ●Staff ●Students

History: Revised- December 16, 2010
Approved – June 11, 2009
First Issued – July 1, 2009

Related Policies:
- *Identity Theft Red Flags and Notice of Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003* [16 C.F.R. § 681]
- *Fair and Accurate Credit Transactions Act of 2003* [Public Law 108-159]

Contact for Info: Information Technology and Telecommunications (910) 672-1910
Office of the Internal Auditors (910) 672-2102
Office of Legal Affairs (910) 672-1145

I. PURPOSE

The Federal Trade Commission's (FTC) Red Flags Rule (Rule) was issued with the underlying goal of detecting, preventing, and mitigating identity theft "in connection with the opening of certain accounts or existing accounts," referred to as "*Covered Accounts*." *Red Flags* are defined by the *Rule* as those events which should alert an organization that there is a risk of identity theft. The *Rule* supplements existing legislation aimed at preventing identity theft through tightened data security by addressing situations where individuals are trying to use another person's identity in order to fraudulently obtain resources or services. Institutions are to identify *Red Flags* to alert and to intervene against the possibility of identity theft.

Fayetteville State University (FSU) is subject to the FTC *Rule* because of the following:

- FSU participates in the Federal Perkins Loan program,
- FSU participates as a school lender in the Federal Family Education Loan Program,
- FSU offers institutional loans to; and
- FSU offers a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

In compliance with the *Rule*, FSU has developed this Policy.

II. DEFINITIONS

The following definitions apply to this policy/program:

A. **Covered Account** is defined as follows:

- Any University sponsored or controlled account that involves having faculty, staff, students, alumni or donors undertake multiple payments or transactions, such as a loan or account that is billed or payable monthly, to include, but not be limited to extension of credit, debit cards, Perkins Loans, the Federal Family Education Loan Program, institutional loans, deposit accounts and scholarship accounts.

- Any other account FSU offers or maintains for which there is a reasonably foreseeable risk to holders of identity theft, such as use of consumer reports for employee background checks or applications for credit.

B. **Identifying Information** is defined as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to:

- 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
- individual identification number
- computer's Internet Protocol address
- bank or other financial account routing code

C. **Identity Theft** is defined as fraud committed or attempted using the *identifying information* of another person without authority.

D. **Red Flag Committee** is defined as the individual designated with primary responsibility for oversight of the Program.

E. **Red Flag** is defined as a pattern, practice, alert or specific activity that indicates the possible existence of identity theft.

F. **Service Provider** is defined as a person or entity that provides a service directly to FSU.

III. IDENTIFICATION AND DETECTION OF RED FLAGS

In compliance with the Rule, FSU's process for detecting and preventing identify theft is as follows:

A. Identification of Red Flags

The FTC requires institutions to identify which *Red Flags*, singly or in combination will be used to detect the possible risk of identity theft. In order to identify relevant red flags, FSU has considered the types of covered accounts it offers or maintains, the methods it provides to open its covered accounts, the methods it provides to access its covered accounts, and its previous experiences with identity theft. Thus, FSU has identified the following red flags in each of the listed categories:

1. Notifications and Warnings from Consumer Reporting Agencies

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on an applicant;
- Notice or report from a credit agency of an active duty alert for an applicant;
- Receipt of a notice of address discrepancy in response to a credit report request; or
- Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

2. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing individual information; or
- Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the individual provides (example: inconsistent birth dates);

- Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (examples: an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another individual;
- An address or telephone number presented that is the same as that of another person;
- When a person fails to provide complete personal identifying information on an application when reminded to do so; or
- When a person's identifying information is not consistent with the information that is on file for the individual.

4. <u>Suspicious Covered Account Activity</u>

- Change of address for an account followed by a request to change the individual's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use;
- Mail sent to the individual is repeatedly returned as undeliverable;
- Notice to FSU that an individual is not receiving mail sent by the University;
- Notice to FSU that an account has unauthorized activity;
- Breach in FSU's computer system's security; or
- Unauthorized access to or use of an individual's account information.

5. <u>Alerts from Others</u>

This may include any notice to FSU from an individual, identity theft victim, law enforcement officer or other person that FSU has opened or is maintaining a fraudulent account for a person engaged in identity theft.

B. Detection of Red Flags

The following procedures shall be utilized in the detection of *Red Flag*s:

1. <u>Student Enrollment</u>

In order to detect any of the *Red Flag*s identified in Section II.A. above that are associated with the ***enrollment of a student***, FSU employees shall

take the following steps to obtain and verify the identity of the person when a new account is created:

- Require that certain identifying information such as name, date of birth, academic records, home address or other identifiers be provided; and
- Verify the individual's identity at the time an identification card (review of driver's license or other government-issued photo identification) issued.

2. Existing Accounts

In order to detect any of the *Red Flags* identified above for an existing covered account, FSU employees shall take the following steps to monitor transactions on an account:

- Verify the identification of individuals if they request information (in person, via telephone, via facsimile, via email);
- Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes; and
- Verify changes in banking information given for billing and payment purposes.
- Verify the identification of individuals if they request new/replacement authentications such as network login or Banner PIN.

3. Consumer ("Credit") Report Requests

In order to detect any of the *Red Flag*s identified above for an employment or volunteer position for which a credit or background report is sought, FSU employees shall take the following steps to assist in identifying address discrepancies:

- Require written verification from an applicant that the address provided by the applicant is accurate at the time the request for the credit/background report is made to the consumer reporting agency; and
- In the event that notice of an address discrepancy is received, verify that the credit/background 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 FSU has reasonably confirmed is accurate.

C. Response to the Identification of Red Flags

When potentially fraudulent activity is detected, FSU employees must act quickly to protect individuals and FSU. At a minimum, the FSU employees shall gather all related documentation, write a description of the situation, and present this information to the *Red Flag Administrator*.

The *Red Flag Administrator* shall convene a meeting of the Red Flag Committee to complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include the following:

- Canceling the transaction;
- Notifying and cooperating with appropriate law enforcement;
- Determining the extent of liability of the University; and/or
- Notifying the actual individual upon whom fraud has been attempted.

D. Mitigation of Risk

Once fraudulent activity is detected, FSU employees shall take one or more of the following steps to prevent and/or mitigate any associated risk to the individual. The extent of the prevention and mitigation actions shall depend on the employee's determination of the degree of risk posed by the *Red Flag*.

- Continue to monitor a covered account for evidence of identity theft;
- Contact the individual or applicant (for which a credit report was run);
- Change any passwords or other security devices that permit access to covered accounts;
- Refuse to open a new covered account;
- Provide the individual with a new individual identification number;
- Notify the Red Flag Committee for determination of the appropriate step(s) to take;
- Notify law enforcement;
- File or assist in filing a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement Network of the United States Department of the Treasury; or
- Determine that no response is warranted under the particular circumstances.

IV. PROTECTION OF IDENTIFYING INFORMATION

A. Electronically Stored Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, FSU employees shall take the following steps with respect to electronically stored identifying information:

- Ensure that its website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing individual account information when a decision has been made to no longer maintain such information;
- Ensure that office computers with access to covered account information are password protected;
- Ensure that laptops are password protected and encrypted;
- Avoid use of social security numbers;
- Ensure the security of the physical facility that contains covered account information;
- Ensure that transmission of information is limited and encrypted when necessary;
- Ensure computer virus protection is up to date; and
- Require and keep only the kinds of individual information that are necessary for University purposes.

B. Security of Hard Copies of Identifying Information

Each employee and contractor performing work for FSU shall comply with the following:

- File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with identifying information shall be locked when not in use.
- Storage rooms containing documents with identifying information and record retention areas shall be locked at the end of each workday or when unsupervised.
- Desks, workstations, work areas, printers and fax machines, and common shared work areas shall be cleared of all documents containing identifying information when not in use.
- Whiteboards, dry-erase boards, writing tablets, and other writing surfaces in common shared work areas shall be erased, removed, or shredded when not in use.
- When documents containing identifying information are discarded, they shall be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense-approved

shredding device. Locked shred bins shall be labeled "Confidential paper shredding and recycling."

V. PROGRAM ADMINISTRATION

A. Oversight

1. Responsibility for developing, implementing and updating this Program lies with the *Red Flag Committee*.
2. The Red Flag Committee shall be responsible for ensuring appropriate training of University 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

FSU employees responsible for implementing the Program and handling covered accounts shall be trained annually under the direction of the Red Flag Committee in the detection of *Red Flag*s and the responsive steps to be taken when a *Red Flag* is detected.

C. Reports

The Red Flag Committee shall report to the Chancellor's Cabinet at least annually on compliance by the University with this Program. The report shall address matters such as the effectiveness of the policies and procedures of the University in addressing the risk of identity theft in connection with the opening of *Covered Accounts* and with respect to existing covered accounts; significant incidents involving identity theft and the FSU's response; and recommendations for material changes to the Program.

D. Program Updates

The Red Flag Committee shall monitor, review, and update this Program at least annually to reflect changes in risks to individuals and the soundness of the University from identity theft. In doing so, the Red Flag Committee shall consider FSU's experiences with identity theft situations, changes in Identity Theft methods, changes in identity theft detection and prevention methods, and changes in FSU's business arrangements with other entities.

ATTACHMENT A

RED FLAG/IDENTIFICATION THEFT PROCESS FLOW