The University of Oklahoma Norman Campus
Administration and Finance Policy
Subject: Identity Theft and the Federal Trade Commission's Red Flags Rule
Effective Date: May 1, 2009

I. Purpose

The purpose of this policy is to develop and document an identity theft prevention program pursuant to the Federal Trade Commission's (FTC's) Red Flags Rule (henceforth Rule), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C.F.R. § 681.2.

Under the Rule, every financial institution and creditor is required to establish an Identity Theft Prevention Program tailored to the size, complexity, and nature of its operation. Each program must contain reasonable policies and procedures to:

A. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the program;
B. Detect Red Flags that have been incorporated into the program;
C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft;
D. Implement and adopt the program with approval from the Board of Regents;
E. Update the program periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft; and
F. Oversee the program through a senior management employee

II. Scope

Universities receiving certain federal grants as well as deferring payments for services must comply with these rules. The Rule applies to all "covered accounts," in which the University of Oklahoma is the "creditor." The Rule also applies to universities that *use consumer reports to conduct credit or background checks on prospective employees or applicants for credit*. These terms are defined below:

Creditors

The Rule defines creditors to include any person or organization who defers payment for services rendered. In its July 2008 guidance, the FTC stated "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

Covered Accounts

The Rule defines covered accounts as a consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly. The FTC's guidance indicates that covered accounts include certain types of arrangements in which an individual establishes a "continuing relationship" with the enterprise, including billing for previous services rendered. Any type of account or payment plan that involves multiple transactions or multiple payments in arrears is likely a covered account. Additionally, any account in which there is a reasonably foreseeable risk of identity theft is included.

The University of Oklahoma Norman Campus has covered accounts in the following areas:

A. Office of the Bursar
B. Office of Financial Aid
C. Office of Collections
D. Goddard Health Center

Identifying Information

The Rule defines identifying information as 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, unique electronic identification number, computer's Internet Protocol address, or routing code.

The University's anti-theft guidelines can be found by visiting http://www.ou.edu/oupd/idtheft3.htm.

III. Identify

In order to identify relevant Red Flags, the University of Oklahoma has considered:

A. The types of accounts it offers and maintains;
B. The methods it provides to open its accounts; and
C. The methods it provides to access its accounts.

The University of Oklahoma has identified the following relevant Red Flags, in each of the categories listed:

Suspicious Documents:

A. Documents provided for identification appear to have been altered or forged.
B. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
C. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
D. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor.
E. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information:

A. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
B. Personal identifying information provided is associated with known fraudulent activity as indicated by internal sources used by the financial institution or creditor. For example:
    1. The address on an application is the same as the address provided on a fraudulent application; or
    2. The phone number on an application is the same as the number provided on a fraudulent application.
C. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
    1. The address on an application is fictitious, a mail drop, or a prison; or
    2. The phone number is invalid, or is associated with a pager or answering service.
D. The SSN provided is the same as that submitted by other persons opening an account or other customers.
E. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
F. The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

G. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

A. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

IV. Detect

In order to detect any of the Red Flags above associated with new or existing accounts, University of Oklahoma personnel working in areas with covered accounts (Bursar, Financial Aid, Collections, Goddard Health Center) will take the following steps to obtain and verify proper identity:

A. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
B. Verify the account holder's identity (for instance, review a driver's license or other identification card);
C. Verify any changes made electronically to personal identifying information by emailing individual faculty, staff, students, and affiliates to alert them of changes made to their accounts. Note: the University of Oklahoma will never solicit personal identifying information through email.

V. Respond

If Red Flags are detected and/or personal identifying information is stolen, the University of Oklahoma will:

A. Work with law enforcement officials to formulate an appropriate response;
B. Monitor accounts for suspicious login attempts;
C. Contact faculty, staff, students, and affiliates via email to verify password changes on all accounts (see C under Section IV, above);
D. Change passwords by request;
E. Refuse to open accounts for persons with suspicious or inadequate identifying information;
F. Find no response is warranted.

VI. Implement

This program was approved by the Board of Regents on March 25, 2009.

VII. Update

This program will be annually reviewed and updated to reflect changes in risks to faculty, staff, students, and affiliates at the University of Oklahoma Norman Campus and any Norman campus programs located at other campuses (such as OU Tulsa Schusterman Norman programs) with respect to Red Flags and identity theft. A committee staffed with designees from each relevant unit affected by the Rule shall provide the Office of Administration and Finance with an annual report no later than December 31st of each year, which will identify:

A. The number of detected identity theft issues
B. The response to and outcome of such issues; and
C. The areas that have been identified as requiring updates or modifications to this policy.

VIII. Oversee

Oversight for this program will be provided by the Vice President for Administration and Finance. He/she shall ensure that the policy is implemented and updated. He/she will also provide the relevant affected units with training concerning these rules.