



UNIVERSITY OF CENTRAL OKLAHOMA

Policy ID: ADM-LEG-27 Minor Revision 4 Status: C

Title: Red Flag Policy

Description: UCO customized identity theft prevention program

Category: Legal Services

Applies to: Staff, Faculty, Student

Contact: [Office of Legal Counsel](#)

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.

Policy Statement: 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:

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. **Implement** and adopt the program with approval from the Board of Regents;
5. **Update** the program periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft; and
6. **Oversee** the program through a designated management employee.

Section I

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 University of Central 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 foreseeable risk of identity theft is included.

Identifying Information

Identifying information is 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, or employer or taxpayer identification number.

Section II

Procedure

1. Identify

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

- The types of accounts it offers and maintains;
- The methods it provides to open its accounts;
- The methods it provides to access its accounts; and
- The prior experience with identity theft.

University of Central Oklahoma has identified the following relevant red flags, in each of the categories listed:

Suspicious Documents:

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

Suspicious Personal Identifying Information:

1. 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.
2. 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.
3. 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.
4. The SSN provided is the same as that submitted by other persons opening an account or other customers.
5. 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.
6. 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.
7. 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 (including consumer reporting agencies or service providers) Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

1. 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.

The Unusual Use Of, Or Other Suspicious Activity Related to a Covered Account.

2. Detect

In order to detect any of the Red Flags above associated with new or existing accounts, University of Central Oklahoma personnel will take the following steps to obtain and verify proper identity:

1. 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;
2. Verify the account holder's identity (for instance, review a driver's license or other identification card).

3. Respond

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

1. Work with law enforcement officials to formulate an appropriate response;
2. Monitor accounts for suspicious login attempts;
3. Comply with requirements of 24 O.S. § 161 et. seq.;
4. Change passwords by request;
5. Refuse to open accounts for persons with suspicious or inadequate identifying information;
6. Find no response is warranted.

5. Update

The program will be reviewed annually and updated to reflect changes in risks to faculty, staff, students, and affiliates of the University of Central Oklahoma, with respect to Red Flags and identity theft. A report will be sent to the Executive Vice-President annually regarding compliance. The reports should address:

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

6. Oversee

Oversight for this program will be provided by The Office of Enrollment Management and UCO Administration. The Departments shall ensure that the policy is implemented and updated. The Departments shall send an annual report to the Executive Vice-President regarding compliance. The Departments will also provide the relevant affected units with training concerning these rules.

Glossary of Terms:

Legal Citation: Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C.F.R. § 681.2.

Campus Links:

FAQs:

Formerly known as:

Approved on: 04/30/2009

Effective date: 05/01/2009

Keyword(s): red, flag, identity, theft, prevention, suspicious

Last review date: 09/02/2011

Date posted: May 11 2009 12:23PM

Modified By:

Date Modified: Sep 2 2011 2:15PM

