UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

Red Flags Rules (Identity Theft) Policy

Policy #505

Source of Authority: Fair Credit Reporting Act, 15 U.S.C. §§ 114 & 315;
16 C.F.R. 681;
N.C.G.S. § 116-34(a);
UNC Code § 502(A)

Revision Authority: Chancellor

History: **First Issued:** February 17, 2011

Related Policies: Fair Credit Reporting Act, 15 U.S.C. §§ 114 & 315;
FTC Red Flag Rules, 16 C.F.R. 681;
Confidential Information Access (IT Security) Policy #501;
Improper Activities Reporting Policy #114;
IT Account Management Policy #503;
Technology Use Policy #508

Responsible Offices: Information Technologies

Effective Date: February 17, 2011

I. Purpose

The purpose of the program is to detect, prevent, and mitigate identity theft in connection with any covered account. This program envisions the creation of policies and procedures in order to achieve these goals

II. Scope

This policy applies to all covered UNCSA accounts as enumerated in this policy.

III. Definitions

A. "**Covered Account**" means either:

1. Any account that constitutes a continuing financial relationship or is designed to permit multiple payments or transactions between the University and a person for a service, such as Perkins Loans, FFELP, institutional loans, HIPAA covered accounts, deposit accounts, scholarship accounts, and the like.
2. Any other account the University offers or maintains for which there is a reasonably foreseeable risk to holders of the account or to the safety and soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. "**Identifying Information**" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person as detailed in the Information Security Policy.

C. "**Identity Theft**" means a fraud committed or attempted using the identifying information of another person without authority.

D. "**Program Administrator**" means the individual designated with primary responsibility for oversight of the Program.

E. "**Red Flag**" means a pattern, practice, alert, or specific activity that indicates possible identity theft.

F. "**Service Provider**" means a person or entity that provides a service directly to the University.

IV. Policy

A. Identification of Covered Accounts

1. In order to ensure compliance with the Fair Credit Reporting Act, the University has compiled a list of covered accounts the University currently administers, offers, or maintains, are listed in this policy's procedures.
2. As the University from time to time may add additional covered accounts, prior to opening or instituting any such account, the Program Administrator shall determine what red flags shall apply to that account.
3. Additionally, at least annually, the Program Administrator shall review all existing accounts to determine if the University has added any covered accounts and, if so, will assign appropriate identification, detection, response, prevention, and mitigation strategies to those accounts.

B. Identification of Red Flags

1. In order to identify relevant Red Flags, the University considers the types of covered accounts and how the University opens, accesses and provides access to its covered accounts, as well as the University's previous experiences with identity theft.
2. Red Flags may be detected while implementing existing account opening and servicing procedures such as: individual identification, caller authentication, third party authorization, and address changes.
3. The University identifies Red Flag events or occurrences as listed below for each of the following categories. However, the list is not exclusive and employees should be alert to other reasonable indicators of attempted or actual identity theft.

a. **Suspicious Documents**

i. Identification document or card that appears to be forged, altered or inauthentic;

ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

iii. Other document with information that is not consistent with existing individual information; and

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

b. **Suspicious Personal Identifying Information**

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

   ii. Identifying Information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application);

   iii. Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;

   iv. Identifying Information presented that is consistent with fraudulent activity (examples: an invalid phone number or fictitious billing address);

   v. Social security number presented that is the same as one given by another individual;

   vi. An address or phone number presented that is the same as that of another person;

   vii. A person fails to provide complete personal Identifying Information on an application when reminded to do so; and

   viii. A person's Identifying Information is not consistent with the information that is on file for the individual.

c. **Suspicious Covered Account Activity**

   i. Change of address for an account followed by a request to change the individual's name;

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

   iii. Account used in a way that is not consistent with prior use;

   iv. Mail sent to the individual is repeatedly returned as undeliverable;

   v. Notice to the University that an individual is not receiving mail sent by the University;

   vi. Notice to the University that an account has unauthorized activity;

   vii. Breach in the University's computer system security; and

   viii. Unauthorized access to or use of individual account information.

d. Alerts from Others (an individual 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.

C. **Program Administration.** The Program Administrator is responsible for developing, implementing, and updating this policy including:

1. ensuring appropriate training of University staff on the Program;
2. reviewing any staff reports regarding the detection of Red Flags
3. reviewing the steps for preventing and mitigating identity theft;

4. determining which steps of prevention and mitigation should be taken in particular circumstances; AND
5. considering periodic changes to the Program.

D. **Staff Training**

University employees responsible for implementing this policy shall be trained 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.

E. **Reports**

1. Staff designated by the Program Administrator shall report to the Program Administrator at least annually on compliance by the University with this Program.
2. The report shall address matters such as:
   a. 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
   b. service provider arrangements;
   c. significant incidents involving identity theft and the University's response; AND
   d. recommendations for material changes to the Program.

F. **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 Program Administrator will 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.

G. **Program Updates**

1. The Program Administrator shall review and update this Program at least annually to reflect changes in risks to individuals and the soundness of the University from Identity Theft.
2. In doing so, the Program Administrator shall consider:
   a. the University's experiences with Identity Theft situations;
   b. changes in Identity Theft methods;
   c. changes in Identity Theft detection and prevention methods; AND
   d. changes in the University's business arrangements with other entities.

V. Revision History

A. February 17, 2011 – Adopted by Board of Trustees as part of UNCSA Policy Manual

UNIVERSITY OF NORTH CAROLINA SCHOOL OF THE ARTS

Red Flag Rules (Identity Theft) Procedures

Procedure #505

I. Current UNCSA Covered Accounts:

A. All financial accounts providing for periodic payments;

B. Certain payroll accounts for which UNCSA manages deductions for services (parking, FLEX accounts, etc.)

C. Student service accounts providing for periodic payments, excluding One Card accounts.

II. Procedures for Detecting Red Flags

A. **Student Enrollment**

1. In order to detect any identified Red Flags identified associated with the enrollment of a student, University personnel shall take the following steps to obtain and verify the identity of the person opening the account:

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

   b. Verify the individual's identity at time of issuance of individual identification card (review of a **valid** driver's license or other **valid** government-issued photo identification).

2. The office overseeing the account shall be responsible for implementing these checks and the Program Administrator shall be informed upon the discovery of any failure to do so.

3. In addition to the above measures, staff will remain alert for Red Flags arising from suspicious documents, suspicious personal identifying information, and suspicious covered activity as noted in these policy and procedures.

B. **Other Covered Accounts**

1. In order to detect any identified Red Flags for a covered account, University personnel shall take the following steps to monitor transactions on an account:

   a. Verify the identification of individuals requesting information (in person, via telephone, via facsimile, or via e-mail);

   b. Verify the validity of requests to change billing addresses by mail or e-mail and provide the individual a reasonable means of promptly reporting incorrect billing address changes; AND

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

2. In addition to the above measures, staff will remain alert for Red Flags arising from suspicious documents, suspicious personal identifying information, and suspicious covered activity as noted in these policies and procedures.

III. Response to Red Flags

A. Employees must act quickly once potentially fraudulent activity is detected.

B. In all cases, the employee must:

1. gather all related documentation;
2. write a description of the situation; AND
3. present this information to the Program Administrator as soon as is practical under the circumstances.

C. The Program Administrator will conduct further investigation if necessary and shall reach a reasonable conclusion regarding the authenticity of the attempted transaction.

D. If a transaction is determined likely to be fraudulent, appropriate actions must be taken immediately including, but not limited to:

1. Canceling the transaction;
2. Notifying and cooperating with appropriate law enforcement;
3. Assessing the University's liability; AND/OR
4. Notifying the actual individual upon whom fraud has been attempted.

IV. Prevention and Mitigation of Identity Theft

A. In addition to the above measures, employees who detect any identified Red Flags shall take one or more of the proscribed steps in consultation with the Program Administrator, depending on the Program Administrator's determination of the degree of risk posed by the Red Flag:

B. **General Prevention & Mitigation Measures**

1. Continue to monitor a covered account;
2. Contact the individual or applicant;
3. Change any passwords or other security devices that permit access to covered accounts;
4. Refuse to open a new covered account;
5. Provide the individual with a new individual identification number;
6. Notify the Program Administrator for guidance and determination of the appropriate step(s) to take; AND/OR
7. Notify law enforcement.

C. **Internal Operating Procedures & Measures to Protect Identifying Information.** The University will take the following steps with respect to its internal operating procedures to protect individual 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 individual account information when appropriate;

3. Ensure that computers with access to covered account information are password protected;
4. Avoid use of social security numbers;
5. Ensure the security of the physical facility that contains covered account information;
6. Ensure that transmission of information is limited and encrypted when necessary;
7. Ensure computer virus protection is up to date;
8. Require and keep only the kinds of individual information that are necessary for University purposes; and
9. Establish appropriate procedures for controlling hard copies containing identifying information from covered accounts.