01.230 IDENTITY THEFT PREVENTION PROGRAM (RED FLAGS)

Authority:	Board of Trustees
History:	Effective May 1, 2009 (approved initially April 24, 2009)
Source of Authority:	16 CFR 681.1 and 16 CFR 681.2
Related Links:	Federal Trade Commission;
Responsible Office:	Business Affairs

I. Program Adoption

As a best practice and using as a guide the Federal Trade Commission's (FTC) Red Flags Rule (Rule), implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, the University of North Carolina at Wilmington (university) developed this Identity Theft Prevention Program (Program). The university is covered under the Rule as a creditor because it offers or maintains certain Covered Accounts, as that term is defined below. After consideration of the size and complexity of the university's operations and account systems, and the nature and scope of the university's activities, the Board of Trustees determined that this Program was appropriate for the university, and moved to approve this Program on April 24, 2009. Enforcement begins on May 1, 2009.

II. Purpose

The purpose of the Program is to detect, prevent, respond and mitigate suspected or real incidents of identity theft in connection with any Covered Account. This program envisions the creation of policies and procedures in order to achieve compliance. The Board of Trustees delegates to the Program Administrator the authority to develop appropriate and necessary policies and procedures.

III. Scope

This Program applies to all university departments and to all Service Providers engaged by the university that perform an activity in connection with one or more Covered Account.

IV. Definitions

A. Covered Account

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 extension of credit, debit cards, Perkins Loans, Federal Family Education Loan Program **(** FFELP), institutional loans, Health Insurance Portability and Accountability Act (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 of Identify Theft to holders of the account or to the safety and soundness of the University, including financial, operational, compliance, reputational or litigation risks, or that use consumer reports for prospective employees and student criminal background checks, institutional debit card applications, and the like.

B. Identifying Information - 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:

1) Name
2) Address
3) Telephone number
4) Social Security Number
5) Date of birth
6) Government-issued driver's license or identification number
7) Alien registration number
8) Government passport number
9) Employer or taxpayer identification number
10) Individual identification number
11) Computer's Internet Protocol address
12) Bank or other financial account routing code

C. Identity Theft - a fraud committed or attempted using the Identifying Information of another person without authority.

D. Program Administrator - the individual designated by the Board of Trustees with primary responsibility for oversight of the Program.

E. Red Flag - a pattern, practice, alert or specific activity that indicates the possible existence of Identity Theft.

F. Service Provider - a person or entity that the university has contracted with to perform an activity or a service in connection with one or more Covered Accounts.

V. Identification of Red Flags

A. In order to identify relevant Red Flags, the university considers 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.

B. 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.

C. The university identifies the following Red Flags in each of the listed categories:

1) Notifications and Warnings from Consumer Reporting Agencies

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

2) Suspicious Documents

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

3) Suspicious Personal Identifying Information

   a) Identifying Information presented that is inconsistent with other information the individual provides (example: inconsistent birth dates);
   b) Identifying Information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application);
   c) Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;
   d) Identifying Information presented that is consistent with fraudulent activity (examples: an invalid phone number or fictitious billing address);
   e) Social security number presented that is the same as one given by another individual;
   f) An address or phone number presented that is the same as that of another person, for whom the individuals are unrelated or not co-roommates;

g) A person fails to provide complete personal Identifying Information on an application when requested to do so;
h) A person's Identifying Information is not consistent with the information that is on file for the individual.

4) Suspicious Covered Account Activity

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

5) Alerts from Others

a) Notice to the university from 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.

VI. Detection of Red Flags

A. Student Enrollment

In order to detect any of the Red Flags identified above 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:

1) Require certain Identifying Information such as name, date of birth, academic records, home address or other identification;
2) Verify the individual's identity at time of issuance of individual 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 shall take the following steps to monitor transactions on an account:

1) Verify the identification of individuals 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 individual 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

In order to detect any of the Red Flags identified above for an applicant for employment or volunteer position or for an applicant for student admission or student field study (including an internship) for which a consumer or background report is sought, university personnel shall take the following steps to assist in identifying address discrepancies:

a. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the consumer report is made to the consumer reporting agency;
b. In the event that notice of an address discrepancy is received, verify that the consumer 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.

VII. Response to Red Flags

A. Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect individuals and the university from damages and loss. At a minimum, the employee must gather all related documentation, write a description of the situation, and present this information to the employee's supervisor. The supervisor must review the information and forward to the Program Administrator or designee.

B. The Program Administrator or designee shall complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

C. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
1) Canceling the transaction;
2) Notifying and cooperating with appropriate law enforcement;
3) Determining the extent of liability of the university;
4) Notifying the actual individual upon whom fraud has been attempted; or
5) File or assist in filing a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement Network, United States Department of the Treasury.

VIII. Prevention and Mitigation of 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 their determination of the degree of risk posed by the Red Flag:

1) Prevent and Mitigate

a) Continue to monitor a Covered Account for evidence of Identity Theft;
b) Contact the individual or applicant (for which a consumer report was conducted);
c) Change any passwords or other security devices that permit access to Covered Accounts;
d) Refuse to open a new Covered Account;
e) Provide the individual with a new individual identification number;
f) Notify the Program Administrator, or designee, for determination of other appropriate step(s) to take; or
g) Determine that no response is warranted under the particular circumstances.

2) Protect Identifying Information

In order 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 individual Identifying Information:

a) Ensure that its website is secure or provide clear notice that the website is not secure;
b) 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;
c) Ensure that office computers with access to Covered Account information are password protected;
d) Ensure that laptops are password protected and encrypted;
e) Avoid use of social security numbers, unless required legally;
f) Ensure the security of the physical facility that contains Covered Account information;
g) Ensure that transmission of information is limited and encrypted when necessary;
h) Ensure computer virus protection is up to date; and
i) Require and keep only the types of individual information that are necessary for university purposes.

IX. Additional Identity Theft Prevention Measures

A. Paper or other Hard Copy Distribution

All employees and Service Providers performing work for the university are required to comply with the following procedures:

1) File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Identifying Information will be locked when not in use.
2) Storage rooms containing documents with Identifying Information and record retention areas will be locked at the end of each workday or when unsupervised.
3) Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing Identifying Information when not in use.
4) Whiteboards, dry-erase boards, writing tablets, and other writing surfaces in common shared work areas will be erased, removed, or shredded when not in use.
5) When documents containing Identifying Information are discarded, they will 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 are labeled "Confidential paper shredding and recycling."

X. Program Administration

A. Oversight

1) Program oversight is delegated to the Vice Chancellor for Business Affairs, who shall serve as the Program Administrator and chair of a university committee created for this purpose. The Program Administrator in consultation with a university committee shall be responsible for the oversight, development, implementation and administration of the Program, such as ensuring appropriate training of university employees on the Program, for reviewing any employee 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.

2) University committee membership shall be comprised of one representative from each university division as designated by the chancellor and vice chancellors. The Program Administrator may appoint other members to the committee.

B. Staff Training

All university employees and their supervisors responsible for implementing the Program are required to attend training under the direction of the Program Administrator or designee in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

C. Reports

Each division representative serving on the committee shall report to the Program Administrator 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 in addressing the risk of Identity Theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts; Service Provider arrangements; significant incidents involving Identity Theft and the university's response; and recommendations for material changes to the Program.

D. Service Provider Arrangements

When 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 signed contract, that Service Providers have such policies and procedures in place; and
2) Require, by signed contract, that Service Providers review and agree to abide by the university's Program and report any Red Flags to the Program Administrator directly in a timely fashion.

E. Program Updates

1) The Program Administrator shall review and update this Program at least annually to reflect changes in risks to individuals of Identity Theft or to the safety and the soundness of the university, including financial, operational, compliance, reputational, or litigation risks. In doing so, the Program Administrator shall 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.
2) Each department having Covered Accounts will review its procedures to ensure compliance with the Program at least annually. Written reports of the review must be submitted to the Program Administrator, through the division representative on the university committee.