

OFFICE OF THE CHANCELLOR
University of New Orleans

Administrative Policy & Procedure
AP 9.01
Effective Date: 05/01/2009

SUBJECT: Identity Theft Prevention Program

PURPOSE: To establish an Identity Theft Program in compliance with the Red Flag rules issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions ACT ("FACTA").

AUTHORITY

Article VII, Section 4, By-Laws and Regulations of the Board of Supervisors of the Louisiana State University System.

OBJECTIVE: Set forth a policy establishing an Identity Theft Prevention Program that is tailored to the size, complexity, and nature of operations at The University of New Orleans.

DEFINITIONS

1. Covered Accounts – Are customer accounts with a monthly payment plan, Perkins Loans, and any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from Identity Theft. *Red Flag regulations 16 Code of Federal Regulations (CFR) § 681.2.*
2. Creditor- An entity that regularly extends, renews, or continues credit. *Red Flag regulations 16 CFR § 681.2.*
3. Identifying Information - Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, (*Red Flag regulations 16 CFR § 681.2*) including:
 - Name and Address
 - Telephone Number
 - Social Security Number
 - Date of Birth
 - Driver's License or Government-issued Identification Number
 - Alien Registration Number
 - Passport Number
 - Employer or Taxpayer Identification Number
 - Unique Electronic Identification Number
 - Internet Protocol Address or Routing Code
 -
6. Identity Theft- A fraud committed using the identifying information of another person. *Red Flag regulations 16 CFR § 681.2.*

7. Program Administrator- The individual designated with primary responsibility for oversight of the program.
8. Red Flag- A pattern, practice, or specific activity that indicates the possible existence of Identity Theft. *Red Flag regulations 16 CFR § 681.2.*

PROGRAM ADOPTION

The University of New Orleans developed this Identity Theft Prevention Program (Program) pursuant to the Federal Trade Commission's (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 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 Louisiana State University and A&M College Board of Supervisors determined this Program was appropriate for the University, and therefore approved this Program on <DATE>. Further, the Board directs the Chancellor to appoint an Identity Theft Program Administrator to oversee the successful implementation and ongoing maintenance of the Program at the University.

FULFILLING REQUIREMENTS OF THE RED FLAGS RULE

Under the Red Flags Rule, the University is required to establish an Identity Theft Prevention Program tailored to its size, complexity and the nature of its operation. The 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; and
4. Ensure the Program is updated periodically to reflect changes in the business environment as well as changes in the risks to customers with regards to Identity Theft.

PROCEDURES

The University of New Orleans has adopted this initial Identity Theft Prevention Program (Program) in compliance with the "Red Flag" rules issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions ACT (FACTA). The University is engaging in activities which are covered by the FACTA Red Flag rules.

1. PREVENTING AND MITIGATING IDENTITY THEFT

A. Distribution of Data. In an attempt to minimize and/or eliminate Identity Theft, employees of the University will use the following steps to ensure proper safeguarding of Identifying Information, whether hard-copy or electronic:

i. Hard-Copy Distribution.

- a. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Identifying Information will be locked when not in use.

- b. Storage rooms containing documents with Identifying Information will be locked at the end of each workday or when unsupervised.
- c. 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.
- d. Shred bins will be kept locked. (Documents may only be destroyed in accordance with the University's records retention policy.)

ii. **Electronic Distribution.**

- a. Identifying Information may be transmitted internally among University units, using approved University e-mail.
- b. Identifying Information will be stored on the University's shared drives which are password protected and accessible only to authorized users.

B. Protect Student 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 student identifying information:

- Ensure that its website is secure;
- Ensure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
- Ensure office computers with access to Covered Account information are password protected;
- Ensure computer virus protection is up to date; and
- Require and keep only the student information that is necessary for University purposes.

All five of these measures are covered within one or more of the following University of New Orleans, University Computing and Communications (UCC) policy; University of New Orleans Administrative Policy (AP); and LSU System Permanent Memoranda (PM):

- UNO IT User Policy
- UNO Information Technology General Use Policies
- UNO Computer Lab Policies
- Modem Pool Policy
- Employee Account Termination
- Proper Use of Technology
- Statement on Social Networking Sites
- Data Classification and Data Security
- Educational Privacy Rights of Students
- Louisiana State University System Information Security Plan

B. Non-Disclosure of Specific Practices. For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the Program Administrator

and to those employees with a need to know. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential and should not be shared with other University of New Orleans employees or the public. The Program Administrator shall inform those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

C. 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 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.

- Require, by contract, that service providers have such policies and procedures in place; and
- Require, by contract, that service providers review the University's Program and report any Red Flags to the Program Administrator or the University employee with primary oversight of the service provider relationship.

2. Identifying Red Flags. In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The University identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

RED FLAG

- Notice of an address discrepancy on a Perkins Loan credit bureau dispute verification.

B. Suspicious Documents

RED FLAGS

- Documents or cards provided for identification appear to be forged, altered or inauthentic;
- Photograph or physical description on the identification on which a person's appearance is not consistent with the person presenting the document;
- Other information on the identification is not consistent with existing on file with the University; and
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

RED FLAGS

- Personal identifying information provided is inconsistent when compared against external information sources used by the University;
- Personal identifying information provided by the customer is inconsistent with personal identifying information provided by the customer;
- Personal identifying information provided is the same as information

- provided on other documents that were found to be fraudulent;
- Personal identifying information provided is of a type commonly associated with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number provided is the same as one given by another customer;
- The address or phone number provided is the same as that of another person;
- A customer fails to provide all required personal identifying information on an application when reminded to do so;
- Personal identifying information provided is inconsistent with the information that is on file for the customer.
- In situations where the University uses a security or challenge question, the customer cannot provide authenticating information beyond what would generally be available from a wallet.

D. Suspicious Covered Account Activity or Unusual Use of Covered Account

RED FLAGS

- Three or more address changes requested on the same account within a 90-day period;
- Mail sent to the account holder is repeatedly returned as undeliverable although transactions continue to occur in connection with the account;
- The University is notified that a customer is not receiving mail sent by the University;
- An account that has been inactive for a reasonably lengthy period of time is used;
- The University is notified of unauthorized access, charges, or transactions in connection with a customer's account.

E. Alerts from Others

RED FLAGS

- The University is notified by a customer, an Identity Theft victim, law enforcement, or any person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

3. DETECTING RED FLAGS. The University's Identity Theft Protection Program's general Red Flag detection practices are described in this document. The Program Administrator will develop and implement specific methods and protocols appropriate to meet the requirements of this Program.

A. New Accounts. In order to detect any of the Red Flags identified above associated with the opening of a new account, University personnel should take the following steps to obtain and verify the identity of the person opening the account:

- Require certain Identifying Information such as name, date of birth, academic records, home address or other identification; and
- Verify the student or employee's identity at the time of issuance/reissuance of a University 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 account, University personnel should take the following steps to monitor transactions with an account:

- Verify the identification of customers if requesting information (in person, via telephone, via facsimile, via email); and
- Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes.

C. Credit Reporting. In order to detect the Red Flag identified above for a Perkins Loan credit bureau dispute verification, University personnel will take the following step to assist in identifying address a discrepancy:

- Verify the dispute verification pertains to a valid borrower account in the Perkins Loan system; and
- Report to the credit bureau an address for the borrower that the University has reasonably confirmed is accurate.

4. RESPONDING TO IDENTITY THEFT. In the event University personnel detect any identified Red Flags, such personnel shall endeavor to act quickly and will take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

- Gather all related documentation and write a description of the situation so the designated authority will have the relevant information available for making a determination;
- Continue to monitor a Covered Account for evidence of Identity Theft;
- Cancel the transaction or account;
- Contact the customer;
- Change any passwords or other security devices that permit access to Covered Accounts;
- Refuse to open a new Covered Account;
- Provide the customer with a new identification number;
- Notify the Program Administrator for determination of the appropriate step(s) to take;
- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

5. RESPONSIBILITIES OF THE PROGRAM ADMINISTRATOR. Responsibility for developing, implementing and updating this Program lies with the Identity Theft Program Administrator. The Program Administrator will be responsible for the following:

- **Training.** 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. Train University staff responsible for implementing the Program shall be trained either by or 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. University staff shall be trained, as necessary, to

effectively implement the Program. University employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program;

- **Periodic Evaluation** of this Program to determine whether all aspects of the program are up-to-date and applicable in the current business environment. In doing so, the Administrator will consider the University's experiences with Identity Theft situations, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program will be updated;
- **Annual Reporting.** Obtaining annual compliance update reports from other University staff with direct Program responsibilities. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving Identity Theft and management's response, and recommendations for changes to the Program.

Timothy P. Ryan
Chancellor