University of Nebraska - Lincoln
Identity Theft Prevention Program

I. Purpose & Scope

This program was developed pursuant to the Federal Trade Commission's (FTC) "Red Flag Rules" promulgated pursuant to the Fair and Accurate Credit Transactions Act (the FACT Act). The University's program, as set forth herein, is designed to prevent, to detect and to mitigate identity theft in connection with the opening of a covered account or with the administration of any new or existing covered accounts within the University.

II. Definitions

"Covered Account" means an account that a creditor offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

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

"Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

"Service Provider" means a person or an entity that provides a service directly to the financial institution or creditor.

III. The "Red Flag Rules" Overview

The "Red Flag Rules," found at 16 CFR § 681.2, require a creditor to periodically determine whether it offers or maintains covered accounts. This is done by conducting a risk assessment. Upon identifying any covered account(s) the creditor is required to develop and to implement a written Identity Theft Prevention Program designed 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 addressed by the program;
3. Respond appropriately to any red flags that are detected to prevent and/or mitigate identity theft; and
4. Ensure that the program is updated periodically to reflect changes in risks from identity theft to the account holders or to the safety and soundness of the creditor.

IV. Covered Accounts Maintained by University of Nebraska - Lincoln

1. Student Accounts
2. Student Loans
3. Patient Accounts

V. Identification of Red Flags

The University considered the following risk factors in identifying the specific red flags applicable to its covered accounts.

1. The types of covered accounts offered and maintained;
2. The methods provided for opening and accessing those accounts;
3. Prior experiences with identity theft; and
4. The size, complexity, nature and scope of the institution and its activities.

For example, changing an address more than once a year or changing a direct deposit account for refunds more than once a year would not be considered a red flag action at the University when done through our authenticated site. However, it might constitute suspicious activity at a financial institution whose account holders do not change residences as often as university students. Each of the red flags mentioned below might be applicable to only certain of the covered accounts administered by the University.

The five types of red flags applicable to covered accounts follow with examples of each.

A. Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. Receipt of a fraud or active duty alert accompanying a consumer credit report;
2. Receipt of a notice of credit freeze provided in response to a request for a consumer report;
3. Receipt of a notice of address discrepancy from a credit reporting agency; or
4. Receipt of a consumer report that indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of the account holder (e.g., recent and significant increase in number of inquiries, unusual number of recently established credit relationships, and/or a material change in the use of credit).

B. Suspicious Documents

1. Documents presented for the purpose of personal identification are incomplete or appear to have been altered, forged or appear to be inauthentic;
2. The photographic and/or physical description on the personal identification is inconsistent with the appearance of the individual presenting the document;
3. Other information contained on the personal identification is inconsistent with information provided by the individual opening a new covered account or when presenting the personal identification for verification;
4. Other information contained on the personal identification is inconsistent with readily accessible information on file with the University; or
5. An application received by the University appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against *external* information sources used by the University (e.g., discrepancy in address);
2. Personal identifying information provided is inconsistent when compared against *internal* information held by University (e.g., discrepancy in address, phone number, or other personal identifying information);
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 University (such as fictitious and/or duplicated phone numbers, addresses or social security numbers);
4. Personal identifying information provided is fictitious and/or the same or very similar to that submitted by others opening an account or holding existing accounts (such as addresses, telephone numbers, bank accounts, and social security numbers);
5. The individual opening a covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete; or
6. Challenge questions used by University to allow individuals to access their covered accounts are answered incorrectly.

D. Unusual Use of, or Suspicious Activity Related to, the Covered Account

1. Shortly following a request to change the address for a covered account, the University receives a suspicious request such as to change the account holder's name or to add authorized users on the account;
2. A covered account that has been inactive for a reasonably lengthy amount of time is used in an unusual manner;
3. Mail sent to the account holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
4. The University is notified that the individual is not receiving paper account statements and those statements are not being returned as undeliverable; or
5. The University is notified of unauthorized changes or transactions in connection with an individual's covered account.

E. 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 University

The University is notified by an individual account holder, a victim of identity theft, a law enforcement entity, or any other person that the University has opened a fraudulent account for a person engaged in identity theft.

VI. Responses to Red Flag Detection(s)

Appropriate action should be taken when red flags are detected to confirm the identity of individuals when they open and/or access their covered accounts. The appropriate action(s) from the list that follows will depend on the particular covered account at issue and the relevant circumstances.

1. Appropriate personal identifying information (e.g., photo identification, date of birth, academic status, user name and password, address, etc.) shall be obtained from the individual account holder prior to issuing a new or replacement identification card, to opening a covered account, or to allowing access to a covered account.
2. When certain changes to a covered account are made online, individuals holding covered accounts shall receive notification to confirm the change was valid and to provide instruction in the event the change is invalid.
3. Suspicious changes made to covered accounts that relate to an account holder's identity, administration of the account, or billing and payment information shall be verified.

Other actions will be taken by University personnel involved in the administration of the covered accounts based on the covered account and the circumstances surrounding the detection of red flags. These actions may include one or more of the following.

1. Monitor a covered account for evidence of identity theft;
2. Contact individual account holder(s);
3. Request additional documentation from the individual account holder to verify identity;
4. Change passwords, security codes and other security devices permitting access to the covered account;
5. Close an existing covered account;
6. Notify law enforcement;
7. Take appropriate steps to modify the applicable process to prevent similar activity in the future;
8. Determine that no response is warranted under the particular circumstances.

VII. Program Administration

A. Approval and Oversight: The University of Nebraska Board of Regents shall be responsible for the initial approval of this program. Authority to implement and to administer the program, and to approve all future revisions to the program, shall be delegated to the Audit Committee of the Board of Regents and to those it deems appropriate.

B. Program Assessment and Update: This program should be reviewed and updated at least annually (and more often if circumstances warrant) by performing a risk assessment of the following factors:

1. Prior experiences with identity theft;
2. Changes in the methods of identity theft;
3. Changes in the method of prevention, detection and mitigation of identity theft;
4. Changes in the covered accounts offered and administered by the University; and
5. Changes in the potential red flags that may arise with respect to the covered accounts.

The assessment should also include a review of the reports required pursuant to Section C below. It should consider any changes in risks from identity theft to individual account holders, as well as to the safety and soundness of the University.

C. Reporting: At least annually, each campus will report to the Operations Analysis Department (a.k.a., Internal Audit Department) of the University regarding its compliance with this program. The report(s) should address material matters relating to the program and should evaluate the effectiveness of the program in addressing risks of identity theft in connection with the opening of covered accounts and the administration of new and existing covered accounts. The report(s) also should evaluate service provider arrangements and the handling of significant instances of identity theft, as well as recommend necessary material changes to the program.

D. Staff Training: University departments are delegated responsibility for the development, implementation and administration of this program with respect to their covered accounts. They should develop and implement plans to train their staffs effectively in the identification, prevention, detection and mitigation of the red flags identified above that are applicable to their specific covered accounts. Staff training related to the administration of the particular covered accounts should be conducted at least annually, and as necessary under the circumstances.

E. Oversight of Service Providers: Responsible University departments are those to which responsibility has been delegated for administering this program with respect to their particular covered accounts. If the University engages a service provider to perform an activity in connection with a covered account, the responsible University department(s) should take steps necessary to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to prevent, to detect, and to mitigate the risk of identity theft.