University of North Dakota

Identity Theft Prevention Program

Effective beginning May 1, 2009

I. PROGRAM ADOPTION

University of North Dakota ("University") 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. This Program was developed in accordance with North Dakota University System (NDUS) Policy 802.7 Identity Theft Prevention.

II. DEFINITIONS AND PURPOSE

A. Red Flags Rule Definitions Used in this Program

> "Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."
>
> A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."
>
> A "Covered Account" includes all student and other customer financial accounts or loans that are administered by the University.
>
> A "Student/Customer" includes enrolled students, students with completed applications, vendors, contractors, customers, faculty, staff, and affiliates.
>
> "Program Administrator" is the individual designated with primary responsibility for oversight of the program.
>
> "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 but not limited to: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, other customer identification numbers, computer's Internet Protocol address, student/customer photographic identification, or routing code.

B. Purpose of the Red Flags Rule

> Under the Federal Trade Commission's Red Flags Rule, the University is required to establish an "Identity Theft Prevention Program" that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

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. Ensure the Program is updated periodically to reflect changes in risks or to the safety and soundness of the student and other customers from Identity Theft.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, 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 Collection Agencies

Red Flags

1. Notice or report from a collection reporting agency of a credit freeze on a student/customer;
2. Notice or report from collection reporting agency of an active duty alert for a student/customer;
3. Receipt of a notice of address discrepancy from a collection reporting agency;
4. Indication from a collection reporting agency of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student/customer information;
4. Application that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the student/customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another student/customer;
6. A person fails to provide complete personal identifying information on an application when reminded to do so;
7. A person's identifying information is not consistent with the information that is on file for the student/customer.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1. Payments stop on an otherwise consistently up-to-date account;
2. Account used in a way that is not consistent with prior use;
3. Mail sent to the student/customer is repeatedly returned as undeliverable, although transactions continue to be conducted in connection with the student's/customer's account;
4. Notice to the University that a student/customer is not receiving mail sent by the University;

5. Notice to the University that an account has unauthorized activity;
6. Unauthorized access to or use of student/customer account information.

E. Alerts from Others

Red Flag

1. Notice to the University from a student, 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.

IV. DETECTING RED FLAGS

In order to detect any of the Red Flags identified above associated with the enrollment of a student or services to a customer, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

A. New Accounts (student enrollment, new employee or other new customers)

Detect

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification;
2. Verify the student, faculty, or staff member's identity at time of issuance of a student, faculty, or staff 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 will take the following steps to monitor transactions on an account:

Detect

1. Verify the identification of students/customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change addresses by mail or email and provide the student/customer a reasonable means of promptly reporting incorrect address changes;
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING 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 the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Contact the student/customer or applicant;
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Do not open a new Covered Account;
5. Provide the student with a new student identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. Determine that no response is warranted under the particular circumstances.

Protect Student/Customer 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:

1. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
2. Avoid use of social security numbers;
3. Require and keep only the kinds of student/customer information that are necessary for University purposes.
4. Employees follow the UND data protection best practices located at http://itsecurity.und.edu/DataProtection/DataProtection.html

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Program Administrator who may be the President of the University or his or her appointee. Other individuals appointed by the President of the University or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for 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.

B. Staff Training and Reports

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.

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.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. 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.