Agenda Item 9.a.(9) ***Action***
September 17, 2009

FEDERAL TRADE COMMISSION RED FLAGS RULES

The Federal Trade Commission (FTC), in conjunction with other related agencies, has issued final rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). These rules require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of certain covered accounts or certain existing covered accounts. In addition, these agencies have issued guidelines to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of the rules. After a number of enforcement delays, the mandatory compliance date for these rules is now set for November 1, 2009. While institutions of higher education are normally not considered banks or traditional financial institutions, the University does hold certain covered accounts, including but not limited to student accounts maintained by the Bursar's Office and the processing of Student Financial Aid applications, for which the FTC has envisioned colleges and universities falling within the scope of these rules.

In preparation for this compliance deadline, representatives from University Legal Services, Registration and Records, Information Technology Services, Student Financial Aid, the Office of the Bursar, Human Resources Services, Internal Audit and Treasury Operations have coordinated to develop an Identity Theft Prevention Program that would be suitable to the University's size, complexity and the nature of its operations. This Program contains reasonable policy and procedure statements in order to identify, detect and respond to relevant "Red Flags." "Red Flags" are indications of possible identity theft such as address discrepancies, name discrepancies on identification and insurance or financial information, presentation of suspicious documents, personal information inconsistent with information already on file, unusual use or suspicious activity related to a covered account, and/or notice from a third party of unusual activity related to that covered account. For this reason, these rules are commonly known as the FTC's Red Flags Rules.

Recommendation: The Red Flags Rules require that the initial written Program be approved by each financial institution's or creditor's governing board or an appropriate committee of said board by no later than November 1, 2009. The University requests that the Board approve the initial written Program with appropriate delegation of oversight, development, implementation and administration of the Program to a designated member of senior management as determined by the President.

Identity Theft Prevention Program

I. Program Adoption

Northern Illinois University ("NIU" or "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 ("FACTA") of 2003. Northern Illinois University adopts this Program to help protect against the risks to the University, its employees, its students, and its customers from data loss and identity theft. These risks are of significant concern to Northern Illinois University and can only be reduced through the combined efforts of each employee and associated service provider. This Identity Theft Prevention Program is operated as an extension and in conjunction with the University's Policy for Fraud Detection and Prevention and other relevant University policies, plans, practices and programs aimed at securing and safeguarding the operational and business functions of the University.

II. Definitions and Program

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; i.e., warning signs of potential Identity Theft.

A "Covered Account" is an account that the University offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. A Covered Account includes Bursar student accounts or loans that are administered by the University, and may impact other customer/commercial accounts depending on the circumstances.

- The "Huskie Bucks Accounts" associated with the NIU OneCard are not considered Covered Accounts since they are pre-paid debit accounts for students, faculty and staff.
- TCF Bank accounts that may be linked to the NIU OneCard are processed and maintained by TCF Bank. That institution's identity theft prevention policies will apply to those accounts.

"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. Examples include, but are 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, computer's Internet Protocol address, bank account numbers or bank routing transit code.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, with the approval of its governing board the University is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. This Program is required to 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 risks to students or to the safety and stability of the student 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 as potential indicators of fraud in each of the listed categories:

A. Alerts, Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;
2. Notice or report from a consumer reporting agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of a fraud or active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity. Such irregular or suspicious account activity may include:
6.
   a. A recent and significantly noticeable increase in the volume of inquiries;
   b. An unusual number of recently established credit relationships;
   c. A material change in the use of credit, especially with respect to recently established credit relationships; or
   d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. Suspicious Documents

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 with existing student information; and
3. Application for service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student provides (e.g., inconsistent birth dates or a lack of correlation between the Social Security number (SSN) range and the date of birth);
2. Identifying information presented that is inconsistent with other sources of information. For example:
   a. The address does not match an address on a loan application or credit report;
   b. Name discrepancy on identification and insurance information; or
   c. The SSN has not been issued or is listed on the Social Security Administration's Death Master File;
3. Identifying information presented that is consistent with known fraudulent activity as indicated by internal or third-party source used by the University (e.g., information shown on other applications that were found to be fraudulent);
4. Identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third party sources used by the University. For example:
   a. The address on an application is fictitious, a mail drop, or a prison; or
   b. The phone number is invalid or is associated with a pager or answering service;
5. Social Security Number presented that is the same as one given by another student or customer or person;
6. An address or phone number presented that is the same as that of another person or submitted by an unusually large number of other customers or persons opening accounts;

7. The customer or person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete; and
8. A person's identifying information is not consistent with the information that is on file for the student.

D. Suspicious Covered Account Activity or Unusual use of Account

1. When using security questions (e.g. mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report;
2. Change of address for an account followed by such things as a request to change the student's name, a request for new, additional, or replacement goods or services, or for the addition of authorized user on the account;
3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example:
   a. Payments stop on an otherwise consistently up-to-date account; or
   b. Account used in a way that is not consistent with prior use;
4. A covered account that has been inactive for a reasonably lengthy period of time is recently used (taking into consideration the type of the account, the expected pattern of usage, and other relevant factors);
5. Mail sent to the student is repeatedly returned as undeliverable, especially if transactions on the account continue to be conducted;
6. Notice to the University that a student is not receiving mail sent by the University;
7. Notice to the University that an account has unauthorized activity;
8. Actual or attempted compromises in the University's computer system security; and
9. Attempted or actual unauthorized access to or use of student account information.

E. Alerts from Others: Notice to the University by a student, customer, a victim of identity theft, a law enforcement authority, or any other person that he/she has opened a fraudulent account for a person engaged in identity theft.

NIU recognizes that this may not be a complete list of the Red Flags associated with maintaining Covered Accounts. Since technology growth is not static, and the efforts of persons who want to commit Identity Theft keep evolving, new Red Flags may arise frequently.

IV. Detecting Red Flags

A. NIU OneCard:

In order to detect any of the Red Flags identified above associated with the initial issuance of an NIU OneCard, University personnel will take the following steps to obtain and verify the identity of the person receiving the identification card:

1. Require that the student be registered for classes; and
2. Verify the student's identity at the time of issuance of student identification card through a review of driver's license, State issued ID, United States Military ID, passport or other appropriate documentation.

B. Student Bursar Accounts and Financial Aid Processing:

Bursar accounts for students are automatically created for students upon admission and enrollment to the institution. In order to detect any of the Red Flags identified above for a Covered Account, University personnel will take the following, reasonable steps to monitor transactions on an account:

1. Verify the identification of students 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 student a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking/financial information given for billing and payment purposes. Depending on the circumstances, an additional verification of the identification of the student may be in order when new billing information is presented to the University.

Students and their parents may qualify for financial aid to support the students' academic pursuits. In addition to the appropriate steps outlined above, University personnel will take the following, reasonable steps to monitor transactions on student financial aid loan processing files in order to detect any of the Red Flags identified above for those files:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
2. Obtain identifying information about and verify the identity of a student or parent who applies for financial aid;
3. Coordinate with external lenders and the U.S. Department of Education when those agencies also identify Red Flags or discrepancies in the information that they respectively hold and what is submitted to them by the University or the applicant during the financial aid loan application process;

NIU recognizes that verification or authentication of the identification of a student/customer can be a complex process when combating attempts at Identity Theft. University Personnel may take additional, reasonable measures beyond those listed here depending upon the circumstances.

C. Consumer ("Credit") Report Requests:

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel in Human Resource Services will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the request report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

V. Preventing and Mitigating Identity Theft

In the event University personnel detect any identified Red Flags, such personnel shall gather all related documentation and prepare a brief description of the situation. Upon detection of a potential Red Flag, this initial investigation must be immediately forwarded to the preparing employee's supervisor. The supervisor will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic. The supervisor may take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Continue to monitor a Covered Account for evidence of Identity Theft;

B. Contact the student, customer or applicant;

C. Change any passwords or other security devices that permit access to Covered Accounts;

D. Not open a new Covered Account;

E. Cancel the current transaction;

F. Provide the student with a new student identification number;

G. Notify the Program Administrator for determination of the appropriate steps to take;

H. Notify and cooperate with law enforcement; or

I. Determine that no response is warranted under the particular circumstances.

If a Red Flag is also associated with an attempted or actual breach of the security of personally identifying information, employees are required to immediately, but not later than two business days after discovery of such Red Flag, report such incident to the ITS Customer Support Center at 815-753-8100 and ask that Information Security & Operations be notified. Other appropriate and reasonable measures may be taken by the supervisor, Program Administrator, or other appropriate University personnel in response to a Red Flag.

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University has implemented other safeguarding and privacy policies, plans, practices and procedures designed to protect student Identifying Information, which include but are not limited to:

- Northern Illinois University Information Security Policy
- NIU Information Security Plan for purposes of complying with the Financial Modernization Act of 1999
- Operating Procedures for complying with the Illinois Personal Information Protection Act
- System Access and Security Policy
- Northern Illinois University Acceptable Use Policy
- Catalog statements on Student Information and Records

VI. Program Administration

A. Oversight

Operational responsibility for developing, implementing and updating this Program lies with a Program Administrator who is designated by the President of the University. 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. Relevant University staff shall be trained, as necessary, to effectively implement the Program. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made. 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.

At least annually or as otherwise requested by the Program Administrator, University staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risks 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.

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.

A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Red Flags Rules and validated by appropriate due diligence, may be considered to be meeting these requirements. It is advisable for NIU employees using external service providers to either obtain a copy of the provider's policy or a statement from the provider stating the existence of the policy and a promise of due diligence.

Any specific requirements should be specifically addressed in the appropriate contract arrangements. University Legal Services are available for consultation and review of specific contractual arrangements that are proposed.

D. 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 those employees with a need to know them. 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 unauthorized NIU employees, contractors 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.

E. Program Updates

The Program Administrator will periodically review and update this Program to determine whether all aspects of the Program are up to date and applicable. In doing so, the Program Administrator will 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. Periodic reviews will also include an assessment of which accounts are covered by this Program. 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 Administrator will update the Program.