Ferris State University

BUSINESS POLICY

TO: All Members of the University Community 2009:08

DATE: May 2009

IDENTITY THEFT PREVENTION PROGRAM

I. BACKGROUND

The risk to the University, and its students, faculty, staff and other constituents from data loss and identity theft is of significant concern to the University and the University should make reasonable efforts to detect, prevent, and mitigate identify theft.

II. PURPOSE

The University has developed this Identity Theft Prevention Program (the "Program") in conformity with the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 in an effort to detect, prevent, and mitigate identify theft in connection with the opening of a "covered account" or any existing "covered account," as defined in Section IV. A. and provide for continued administration of the Program. The Program is further intended to help protect students, faculty, staff, and other constituents and the University from damages related to the fraudulent activity of identity theft.

This Program will:

A. Identify patterns, practices, or specific activities ("Red Flags") that indicate the possible existence of identity theft with regard to new or existing covered accounts;
B. Detect Red Flags that have been incorporated into the Program;
C. Respond appropriately to any Red Flags that are detected under the Program;
D. Ensure periodic updating of the Program, including reviewing the accounts that are covered and the identified Red Flags that are part of the Program; and
E. Promote compliance with state and federal laws and regulations regarding identity theft protection.

III. SCOPE

This Identity Theft Prevention Program applies to students, faculty, staff and other constituents at the University.

IV. DEFINITIONS

A. Covered Accounts

For the purpose of the University's Identity Theft Prevention Program, a "covered account" includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing account maintained by the University for its students, faculty, staff and other constituents that meets the following criteria is covered by this program:

1. Accounts for which there is a reasonable foreseeable risk of identity theft; or
2. Accounts for which there is a reasonable foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. Confidential Information

For the purpose of the University's Identity Theft Prevention Program, "confidential information" includes, but is not limited to, the following items whether stored in electronic or printed format.

1. Credit card information, including:
   a. Credit card number (in part or whole)
   b . Credit card expiration date
   c. Cardholder name
   d. Cardholder address
2. Tax identification numbers, including:
   a. Social Security number
   b. Business identification number
   c. Employer identification number
3. Other information commonly used in identity theft

   The following information even though it may otherwise be considered public or proprietary, is often used in conjunction with confidential information to commit fraudulent activity such as identity theft:

   a. Payroll information, including among other information:
      i. Pay checks
      ii. Pay stubs
   b. Flexible benefits plan check requests and associated paperwork
   c. Medical information for any employee or customer, including but not limited to:

i. Doctor names and claims
ii. Insurance claims
iii. Prescriptions
iv. Any related personal medical information

d. Other personal information belonging to students, faculty, staff and other constituents, examples of which include:
i. Date of birth
ii. Address
iii. Phone numbers
iv. Maiden name
v. Names
vi. Campus Wide ID Number

C. Red Flag

For the purpose of the University's Identity Theft Prevention Program, "Red Flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

V. RED FLAG PATTERNS/PRACTICES/ACTIVITIES

The following Red Flags are potential indicators of fraud. Any time a Red Flag, or a situation closely resembling a Red Flag, is apparent, it should be investigated for verification.

A. Credit Reports: examples of these Red Flags include the following:
1. A fraud or active duty alert included with a consumer report;
2. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
3. A notice of address discrepancy from a consumer reporting agency as defined in 334.82(b) of the Fairness and Accuracy in Credit Transactions Act; and
4. A consumer report that indicates a pattern of activity inconsistent with the history and usual pattern or activity of an applicant or customer, such as:
a. A recent and significant 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: examples of these Red Flags include the following:

1. Documents provided for identification that appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student, faculty, staff and other constituent presenting the identifications;
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or student, faculty, staff, and other constituent presenting the identifications;
4. Other information on the identification is not consistent with readily accessible information that is on file with the University; and
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious personally identifying information: examples of these Red Flags include the following:
    1. Personally identifying information provided is inconsistent when compared against external information sources used by the University;
    2. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University;
    3. Personally identifying information provided is a type commonly associated with fraudulent activity as indicated by internal or third party sources used by the University;
    4. The SSN provided is the same as that submitted by another student, faculty, staff, or constituent;
    5. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.
    6. The person opening the covered account fails to provide all required personally identifying information on an application or in response to notification that the application is incomplete;
    7. Personally identifying information provided is not consistent with personal identifying information that is on file with the University; and
    8. When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. Unusual use of, or suspicious activity related to, the covered account: examples of these Red Flags include the following:
    1. Shortly following the notice of a change of address for a covered account, the University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account;

2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments;
3. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
4. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors);
5. Mail sent to the student, faculty, staff, or other constituent is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
6. The University is notified that the student, faculty, staff, or other constituent is not receiving paper account statements;
7. The University is notified of unauthorized charges or transactions in connection with a covered account;
8. The University receives notice from students, faculty, staff, or other constituents, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University; and
9. The University is notified by a student, faculty, staff, or other constituent, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

VI. IDENTITY THEFT PREVENTION

All University personnel and contractors performing work for the University shall comply with the following requirements:

A. Covered Accounts

1. Detection of Red Flags in connection with the opening of covered accounts as well as existing covered accounts shall be made through such methods as:
   a. Obtaining and verifying identity
   b. Authenticating customers
   c. Monitoring transactions

B. Hard Copy Distribution

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with confidential information must be locked when not in use.
2. Storage rooms containing documents with confidential information and record retention areas must 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 must be cleared of all documents containing confidential information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas containing confidential information must be erased, removed, or shredded when not in use.
5. University records may only be destroyed in accordance with the University's records retention policy and applicable law.

C. Electronic Distribution
    1. Internally, confidential information may be transmitted using approved institutional e-mail. All confidential information must be encrypted when stored in an electronic format.
    2. Any confidential information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail: *"This message may contain confidential and/or proprietary information and is intended for the person/entity to which it was originally addressed. Any use by others is strictly prohibited."*

D. Consumer Reports
    1. Compare the information in the consumer report provided by the consumer reporting agency with information the University:
        a. Obtains and uses to verify the consumer's identity;
        b. Maintains in its own records, such as applications, change of address notifications, or other customer account records; or
        c. Obtains from third-party sources; or
    2. Verify the information in the consumer report provided by the consumer reporting agency with the consumers.

E. Application of other Laws and University Policies
    1. University personnel should make reasonable efforts to secure confidential information to the proper extent. Furthermore, this section should be read and applied in conjunction with the Family Education Rights and Privacy Act ("FERPA"), the Michigan Public Records Act, and other applicable laws and University policies. If any employee is uncertain of the confidentiality of a particular piece of information, he/she should contact the designated authority.

VII. RESPONDING TO RED FLAGS

A. Once a Red Flag, or potential Red Flag, is detected, the University should endeavor to act quickly as a rapid appropriate response can protect students, faculty, staff, and other constituents and the University from damages and loss.

1. Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the Associate Vice President of Finance.
2. The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

B. If a transaction is determined to be fraudulent, appropriate actions should be taken immediately. Actions may include:
    1. Canceling the transaction;
    2. Contacting the customer;
    3. Change Account Number;
    4. Change Passwords;
    5. Suspend Activity on Account;
    6. Notifying and cooperating with appropriate law enforcement;
    7. Determining the extent of liability of University;
    8. Notifying the student, faculty, staff, or other constituent that fraud has been attempted; and
    9. No response is warranted.

VIII. PERIODIC UPDATES TO THE IDENTITY THEFT PREVENTION PROGRAM

A. At periodic intervals as deemed necessary by the University, the Program should be re-evaluated to determine whether all aspects of the Program are up- to-date and applicable in the current operational environment.

B. Periodic review will include an assessment of which accounts are covered by the Program.

C. As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate.

D. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the University and its students, faculty, staff, and other constituents.

IX. PROGRAM ADMINISTRATION

A. Involvement of Management
    1. The University's Board of Trustees has approved this Identity Theft Prevention Program.
    2. Operational responsibility for the Program, including but not limited to the oversight, development, implementation, and administration of the Program in conformity with applicable law, and implementation of any necessary changes to the Program, is

delegated to the Associate Vice President of Administration and Finance.

B. Employee Training

1. Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the Vice President of Administration and Finance, or a designee that may come into contact with accounts or personally identifiable information that may constitute a risk to the University or its students, faculty, staff, and other constituents.
2. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

C. Oversight of Service Provider Arrangements

1. It is the responsibility of the University to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Red Flag Rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

Jerry Scoby
Vice President for Administration
and Finance

Contact: Associate Vice President for Finance

Bpl0908.doc