RESOLUTION OF
LAKE SUPERIOR STATE UNIVERSITY
BOARD OF TRUSTEES

ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM
FOR LAKE SUPERIOR STATE UNIVERSITY

WHEREAS, The Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, requires rules regarding identity theft protection to be promulgated and adopted jointly by the Office of the Comptroller of the Currency, Treasury; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; the Office of Thrift Supervision, Treasury; the National Credit Union Administration; and the Federal Trade Commission; and

WHEREAS, Those rules were to take effect November 1, 2008; The FTC extended the enforcement date to August 1, 2009, and requires certain financial institutions and creditors to implement an identity theft prevention program;

WHEREAS, 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 Board of Trustees has determined that the University should make reasonable efforts to detect, prevent, and mitigate identify theft; and

WHEREAS, The Board of Trustees has determined that the proposed Identity Theft Prevention Program is in the best interest of the University and its students, faculty, staff, and other constituents.

NOW, THEREFORE BE IT RESOLVED by the Board of Trustees for Lake Superior State University meeting in Sault Ste. Marie, MI on July 10, 2009 that:

1. the "Identity Theft Prevention Program" attached hereto as Exhibit A is hereby approved; and

2. the Chief Financial Officer of the University is hereby delegated operational responsibility of the Program, including but not limited to oversight, development, implementation, and administration of the Program; approval of needed changes to the Program; and implementation of needed changes to the Program.

Adopted by unanimous roll call vote of the Board of Trustees on this 10th day of July, 2009.

_____ _____

W.W. LaJoie, Chair Tony McLain, President

EXHIBIT A

IDENTITY THEFT PREVENTION PROGRAM

SECTION 1: 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. The University has not experienced an actual case of identity theft thus far. However, several claims of forgery have occurred and the responsible office investigated and resolved appropriately. In all cases, actual identity theft had not occurred.

SECTION 2: COVERED ACCOUNTS

The Red Flags Rule defines the terms "creditor" and "covered accounts" broadly. A "creditor" under the Red Flags Rule includes any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. Although the FTC, in many contexts, does not have jurisdiction over not-for-profit entities, it has taken the position that not-for-profits are subject to FTC jurisdiction when they engage in activities in which a for-profit entity would also engage. In its July 2008 guidance, the FTC stated "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

Activities that cause Lake Superior State University to be considered a "creditor" under the Red Flags Rule include:

- participating in the Federal Perkins Loan program,
- participation in the Department of Human Services Nursing Loan program,
- participating as a school lender in the Federal Family Education Loan Program,
- offering institutional loans to students or
- offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

SECTION 3: SCOPE

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

SECTION 4: IDENTITY THEFT PREVENTION

4.A: Confidential and Personally Identifiable Information for the Purpose of the University's Identify Theft Protection Program

4.A.1: Definition of Confidential and Personally Identifiable Information

Confidential and personally identifiable information includes, but is not limited to, the following items whether stored in electronic or printed format.

4.A.1.a: Credit card information, including:

1. Credit card number (in part or whole)
2. Credit card expiration date

4.A.1.b: Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification number

4.A.1.c: Banking information, including:

1. Bank Name
2. Bank Routing Number
3. Account Number

4.B.: Other Information Commonly Used in Identity Theft

4.B.1: 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:

1. Date of birth
2. Address
3. Phone numbers
4. Account holder name (including maiden name)
5. Customer number

4.C: Hard Copy Distribution

All University personnel shall comply with the following requirements:

1. Offices containing 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.

4.D: Electronic Distribution

1. Confidential Information in an electronic format must be protected from unauthorized access or disclosure at all times.

2. All e-mails containing Confidential Information should include the following statement:

   "This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

4.E.: Application of Other Laws and University Policies

University personnel will 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 an employee is uncertain of the confidentiality of a particular piece of information, he/she should contact the University's Chief Financial Officer, or a designee of the Chief Financial Officer, as set forth in Section 8.A.2.

SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION EFFORTS

5.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 reasonably foreseeable risk of identity theft; or

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

5.B: Red Flags

5.B.1: 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 must be investigated for verification.

1. **Alerts, notifications, or warnings from a consumer reporting agency.** Examples of these Red Flags include the following:

    a. A fraud or active duty alert included with a consumer report;

    b. 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

2. **Suspicious documents.** Examples of these Red Flags include the following:

    a. Documents provided for identification that appear to have been altered or forged;

    b. The photograph or physical description on the identification is not consistent with the appearance of the student, faculty, staff, and other constituent presenting the identification;

    c. Other information on the identification is not consistent with readily accessible information that is on file with the University; and

3. **Suspicious personally identifying information.** Examples of these Red Flags include the following:

    a. Personally identifying information provided is inconsistent when compared against external information sources used by the University;

    b. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University;

    c. Personally identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University;

    d. The SSN provided is the same as that submitted by another student, faculty, staff, or constituent;

    e. Personally identifying information provided is not consistent with personal identifying information that is on file with the University; and

4. **Unusual use of, or suspicious activity related to, the covered account.** Examples of these Red Flags include the following:

    a. 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;

    b. The University is notified that the student, faculty, staff, or other constituent is not receiving paper account statements;

    c. The University is notified of unauthorized charges or transactions in connection with a covered account;

    g. 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

SECTION 6: RESPONDING TO RED FLAGS

6.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.

6.A.1: The University should quickly gather all related documentation, write a description of the situation, and present this information to the University's Chief Financial Officer, or a designee of the Chief Financial Officer, as set forth in Section 8.A.2, for determination.

6.B: If a transaction is determined to be fraudulent, appropriate actions should be taken immediately. Actions may include:

1. Canceling the transaction;

2. Notifying the appropriate credit reporting agency if it is a reported account;

3. Notifying and cooperating with appropriate law enforcement;

4. Determining the extent of liability of the University; and

5. Notifying the student, faculty, staff, or other constituent that fraud has been attempted.

SECTION 7: PERIODIC UPDATES TO THE IDENTITY THEFT PREVENTION PROGRAM

7.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.

7.B: Periodic reviews will include an assessment of which accounts are covered by the Program.

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

7.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.

SECTION 8: PROGRAM ADMINISTRATION

8.A: Involvement of management

8.A.1: Establishment of the Identity Theft Prevention Program is the responsibility of the University's Board of Trustees. The Board's approval of the initial plan must be appropriately documented and maintained.

8.A.2: Operational responsibility of the Program, including but not limited to the oversight, development, implementation, and administration of the Program, approval of needed changes to the Program, and implementation of needed changes to the Program, is delegated to the University's Chief Financial Officer, or a designee of the Chief Financial Officer.

8.B: Employee training

8.B.1: Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the University's Chief Financial Officer, or a designee of the Chief Financial Officer, that the employee 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.

8.B.2: The University's Human Resources office is responsible for ensuring that identity theft training is documented for all employees for whom it is required.