MINNESOTA STATE COLLEGES AND UNIVERSITIES
BOARD OF TRUSTEES

Agenda Item Summary Sheet

Committee: Finance, Facilities and Technology **Date of Meeting:** March 18, 2009

Agenda Item: Identity Theft Prevention Program

☐ Proposed Policy Change	☐ Approvals Required by Policy	☒ Other Approvals	☐ Monitoring

☐ Information

Explain why item is on the Board agenda: The Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires the Federal Trade Commission (FTC) to development and implement regulations to mitigate incidents of identity theft. The FTC regulations require Board approval of the initial written Identity Theft Program; subsequent Program maintenance may be delegated to a committee or senior management, and the recommended motion contains delegation language.

Scheduled Presenter(s): Laura M. King, Vice Chancellor—Chief Financial Officer
Tim Stoddard, Associate Vice Chancellor, Financial Reporting

Outline of Key Points: The FTC issued the required regulations in November 2007; this program is a direct response to FTC regulatory requirements calling for enforcement of such a program beginning on May 1, 2009.

The FTC regulatory provisions are called the "Red Flags Regulations." Unlike many of the other laws and regulations that address data security and data privacy and at least in part look to protect against identity theft, the Red Flags Regulations seek to prevent one who has stolen an identity or is in the process of stealing an identity from being successful in committing a fraudulent act. The program and efforts under the program are intended to provide additional efforts aimed at detection and prevention of fraudulent activity directed against the System and its students and employees.

Background Information: The FTC regulations originally contained a November 1, 2008 enforcement date. There was a great deal of uncertainty within Higher Education and other not-for-profit organizations regarding applicability of the regulations. In October of 2008, the FTC addressed this uncertainty by making it clear that not-for-profit organizations were indeed subject to the regulations to the extent they engaged in covered activities. The FTC granted a six month extension, from November 1, 2008 to May 1, 2009, to the effective FTC enforcement date.

BOARD OF TRUSTEES
MINNESOTA STATE COLLEGES AND UNIVERSITIES

BOARD ACTION
Identify Theft Prevention Program

BACKGROUND

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires the Federal Trade Commission (FTC) to develop and implement regulations to mitigate incidents of identity theft. The FTC issued the required regulations in November 2007. The Identify Theft Prevention Program is a direct response to FTC regulatory requirements calling for enforcement of such a program beginning on May 1, 2009.

The FTC regulations originally contained a November 1, 2008 enforcement date. There was a great deal of uncertainty within Higher Education and other not-for-profit organizations regarding applicability of the regulations. In October of 2008, the FTC addressed this uncertainty by making it clear that not-for-profit organizations were indeed subject to the regulations to the extent they engaged in covered activities. The FTC granted a six month extension, from November 1, 2008 to May 1, 2009, to the effective FTC enforcement date.

The FTC regulatory provisions are called the "Red Flags Regulations." Unlike many of the other laws and regulations that address data security and data privacy and at least in part look to protect against identity theft, the Red Flags Regulations seek to prevent one who has stolen an identity or is in the process of stealing an identity from being successful in committing a fraudulent act. The regulations look to subject organizations to identify red flags that single out suspicious circumstances and develop processes to protect against possible fraudulent activity when red flags are triggered. The program and efforts under the program are intended to provide additional efforts aimed at detection and prevention of fraudulent activity directed against the System and its students and employees.

The FTC regulations require Board approval of the initial written Identity Theft Program; subsequent Program maintenance may be delegated to a committee or senior management, and the recommended motion contains delegation language. Responsibility for Program updates will reside with an Identity Theft Prevention Program Committee with members appointed by the Vice Chancellor—Chief Financial Officer. Members of this committee will be drawn from the group of college, university and Office of the Chancellor program administrators.

The Program conforms to FTC regulatory requirements. It will be necessary for the Office of the Chancellor and each college and university to develop and implement customized written procedures as appropriate to address local operations having a reasonable risk of identity theft fraud. Further, the committee of program administrators mentioned above will periodically share and communicate practices, training resources and otherwise further the system's efforts to prevent identity theft fraud.

RECOMMENDED COMMITTEE ACTION:
The Finance, Facilities and Technology Committee recommends that the Board of Trustees adopt the following motion.

RECOMMENDED MOTION:
The Board of Trustees approves the Identity Theft Prevention Program and delegates to the Vice Chancellor-Chief Financial Officer authority to maintain and update the Program as may be necessary to address regulatory changes, system operational changes and make other reasonable changes enhancing Program clarity and effectiveness consistent with regulatory requirements.

Date Presented to the Board: March 18, 2009

Minnesota State Colleges and Universities
Identity Theft Prevention Program

Part 1. Purpose.

This program establishes the requirements and guidelines of the Minnesota State Colleges and Universities Identity Theft Prevention Program. It is the responsibility of each college and university and the Office of the Chancellor to develop specific, customized procedures for identifying, detecting, preventing, and mitigating Identity Theft fraud.

Part 2. Definitions.

A. Red Flags Rule Definitions Used in this Program

Subpart A. System. System, or Minnesota State Colleges and Universities System, means the Board of Trustees, the Office of the Chancellor, the state colleges and universities, and any part of combination thereof.

Subpart B. Identity Theft. Identity Theft is a fraud committed or attempted using the identifying information of another person without authority.

Subpart C. Red Flag. Red Flag is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Subpart D. Program Administrator. Program Administrator is the individual designated with primary responsibility for the program at each College and University and at the Office of the Chancellor.

Subpart E. Covered Account. Covered Account is an account that a College, University, or Office of the Chancellor offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions or any other account that the College, University, or Office of the Chancellor maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College, University, or Office of the Chancellor from Identify Theft.
Examples of Covered Accounts may include student loans, particularly with overage payments, Perkins loans, deferment of tuition payments, emergency loans, or other consumer accounts that involve multiple payments or transactions.

Subpart F. Identifying Information. 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: 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, or routing code.

Part 3. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, each College, University and the Office of the Chancellor is required to establish an Identity Theft Prevention Program tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Identify Theft Prevention 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 from Identity Theft.

The Program shall, as appropriate, incorporate existing polices and procedures that control reasonably foreseeable risks.

Part 4. Identification of Red Flags.

In order to identify relevant Red Flags, each College, University, and the Office of the Chancellor must consider the types of covered 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 System identifies the following Red Flags in each of the listed categories:

Subpart A. Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;

2. Notice or report from a credit agency of a credit freeze on an applicant;

3. Notice or report from a credit agency of an 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.

Subpart 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 presenting the document;

3. Other document with information that is not consistent with existing student information; and

4. Application for service that appears to have been altered or forged.

Subpart C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student 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;

6. A person fails to provide complete personal identifying information on an application when reminded to do so; and

7. A person's identifying information is not consistent with the information that is on file for the student.

Subpart D. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the student's name;

2. Payments stop on an otherwise consistently up-to-date account;

3. Account is used in a way that is not consistent with prior use;

4. Mail sent to the student is repeatedly returned as undeliverable;

5. Notice to the College, University, or Office of the Chancellor that a student is not receiving mail sent by the College, University, or Office of the Chancellor;

6. Notice that an account has unauthorized activity;

7. Breach in the College, University, or Office of the Chancellor's computer system security; or

8. Unauthorized access to or use of the student's account information.

Subpart E. Alerts from Others

Notice from a student, Identity Theft victim, law enforcement or other person that the College, University, or Office of the Chancellor has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Part 5. Detecting Red Flags.

Subpart A. Student Enrollment

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

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and

2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

Subpart B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, College, University, or Office of the Chancellor personnel will take the following 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 information given for billing and payment purposes.

Subpart 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, the College, University, or Office of the Chancellor 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 requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

Part 6. Preventing and Mitigating Identity Theft.

In the event the College, University or the Office of the Chancellor detect any identified Red Flags, the College, University or the Office of the Chancellor shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

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

2. Contact the student or applicant (for which a credit report was run);

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

4. 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 File or assist in filing a suspicious activities report; or

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

Part 7. Staff Training and Reports

System personnel 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. College, University, and Office of the Chancellor personnel are expected to notify their Program Administrator once they become aware of an incident of Identity Theft. At least annually or as otherwise requested by the Identify Theft Prevention Program Committee, Program Administrators shall report on compliance with the Program. The report will address such issues as effectiveness of the guidance in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft, and recommendations for changes to the Program.

Part 8. Service Provider Arrangements

In the event the College, University or Office of the Chancellor engages a service provider to perform an activity in connection with one or more Covered Accounts, the College, University or Office of the Chancellor must 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 the service provider has such policies and procedures in place; and

2. Require, by contract, that the service provider review the System's Program and report any Red Flags to the responsible Program Administrator or the College, University or Office of the Chancellor employee with primary oversight of the service provider relationship.