College Policy 7.10

Identity Theft Prevention Program

Part 1. Purpose

This Program establishes the requirements and guidelines of the Minneapolis Community and Technical College Identity Theft Prevention Program. The college is implementing specific, customized procedures for identifying, detecting, preventing, and mitigating Identity Theft fraud.

Part 2. Definitions

Red Flag Rule Definitions Used in This Program

Subpart A. College

College is Minneapolis Community and Technical College.

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

Program is the Identity Theft Prevention Program implemented by the college.

Subpart E. Program Administrator

Program Administrator is the individual designated with primary responsibility for the Program. The Program Administrator at the college is the Director of Public Safety.

Subpart F. Covered Accounts

Covered Account is an account that the college offers or maintains primarily for personal, family or household purposes that involves or is designated to permit multiple payments or transactions or any other account that the college maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the college from Identity 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 G. 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 number.

Part 3. Fulfilling Requirements of the Red Flag Rule

In compliance with the Minnesota State Colleges and Universities Red Flag Rule, the college has established an Identity Theft Prevention Program in order to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Identity Theft Prevention Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are deleted to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically to reflect changes in risk from Identity Theft.

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

Part 4. Identification of Red Flags

In order to identify relevant Red Flags, the college has considered the types of covered accounts offered and maintained, methods provided to open accounts, methods provided to access accounts, and previous experiences with Identity Theft. The college identifies the following Red Flags in each of the listed categories:

Subpart A. Notification 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 in 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 that a student is not receiving mail sent by the college;
6. Notice that an account has unauthorized activity;
7. Breach in the college'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 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 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 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 addressed 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 employee or volunteer position for which a credit or background report is sought, the college 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 college has reasonably confirmed is accurate.

Part 6. Preventing and Mitigating Identity Theft

In the event the college detects any identified Red Flags, the college 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

College 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 personnel are expected to notify the Program Administrator once they become aware of an incident of Identity Theft. At least annually or as otherwise requested by the Minnesota State Colleges and Universities Identity Theft Prevention Program Committee, the Program Administrator 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 engages a service provider to perform an activity in connection with one or more Covered Accounts, the college 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 the service provider has such policies and procedures in place;
2. Require, by contract, that the service provider review the college's Program and report any Red Flags to the responsible Program Administrator or the college employee with primary oversight of the service provider relationship.

Date of Adoption: 8/11/2009

Date of Implementation (if different from from adoption date):

Date of Last Review: 8/11/2009

Date and Subject of Revisions: