

PROCEDURE MEMORANDUM

TO: MCC Staff

FROM: Office of the President

SUBJECT: Identity Theft Prevention Program “Red Flags Rule”

DATE: April 28, 2009

PURPOSE: To comply with the Federal Trade Commission’s (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

SCOPE: This procedure applies to all full and part-time faculty and staff working with records at the college.

GENERAL PRINCIPLES:

The identity theft ‘red flags rule’ requires creditors who enter into business arrangements that meet the definition of “covered account” to establish an identity theft program. Although the risk of identity theft is low at MCC, implementation of a prevention program is in the best interest of our students, employees and others that we serve.

1. **Definitions:**

- A. **“Account”** means a continuing relationship established by a person with MCC to obtain a product or service for personal, family, household, or business purposes. Account includes, but is not limited to::
- 1) An extension of credit, such as the purchase of property or services involving a deferred payment,
 - 2) A deposit account.
- B. **“Covered Account”** means:
- 1) An account that MCC offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. Examples could include credit or debit card accounts if the cards are issued by the institution, certain student loan accounts, telephone accounts, utility accounts, and accounts for the payment of tuition, fees or other charges over time;
 - 2) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and

soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

- C. **“Customer”** means a person that has a covered account with MCC.
- D. **”Identity Theft”** means a fraud committed or attempted using the identifying information of another person without authority.
- E. **“Identifying Information”** means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any
 - 1) Name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification;
 - 2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
 - 3) Unique electronic identification number, address, or routing code;
 - 4) Telecommunication identifying information or access device (as defined in 18 USC 1029(e)).
- F. **“Red Flag”** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- G. **“Service Provider”** means a person who provides a service directly to MCC.

2. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the College 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:

- A. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
- B. Detect Red Flags that have been incorporated into the Program;
- C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft;
- D. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from Identity Theft.

3. Identification of Red Flags

In order to identify relevant Red Flags, MCC 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. MCC identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies Red Flags

- 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;
- 5) Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents Red Flags

- 1) Identification documents or cards that appear to be forged, altered or inauthentic;
- 2) Identification documents or cards on which a person's photograph or physical description is not consistent with the person presenting the document;
- 3) Other documents with information that is not consistent with existing student information;
- 4) Applications for service that appear to have been altered or forged.

C. Suspicious Personal Identifying Information Red Flags

- 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) An address or phone number presented that is the same as that of another person;
- 7) A person fails to provide complete personal identifying information on an application when reminded to do so;
- 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 Red Flags

- 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 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 MCC that a student is not receiving mail sent by MCC;
- 6) Notice to MCC that an account has unauthorized activity;
- 7) Breach in MCC's computer system security;
- 8) Unauthorized access to or use of student account information.

E. Alerts from Others Red Flag

- 1) Notice to MCC from a student, Identity Theft victim, law enforcement or other person that MCC has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

4. Detecting Red Flags

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, MCC personnel 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;

- 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).

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, MCC 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;
- 3) Verify changes in banking information given for billing and payment purposes.

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, MCC personnel 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;
- 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 MCC has reasonably confirmed is accurate.

5. Preventing and Mitigating Identify Theft

In the event MCC personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Prevent and Mitigate

- 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 (“SAR”);
- 9) Determine that no response is warranted under the particular circumstances.

B. Protect Student Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, MCC will take the following steps with respect to its internal operating procedures to protect student identifying information:

- 1) Ensure that its website is secure or provide clear notice that the website is not secure;
- 2) Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
- 3) Ensure that office computers with access to Covered Account information are password protected;
- 4) Avoid use of social security numbers;
- 5) Ensure computer virus protection is up to date;
- 6) Require and keep only the kinds of student information that are necessary for MCC purposes.

6. Program Administration

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) for MCC. The Committee is headed by a Program Administrator who may be the President of MCC or his or her appointee.

Two or more other individuals appointed by the President of MCC or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of MCC 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

MCC 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. MCC staff shall be trained, as necessary, to effectively implement the Program. MCC employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of MCC's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, MCC 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 risk 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 MCC engages a service provider to perform an activity in connection with one or more Covered Accounts, MCC 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;
- 2) Require, by contract, that service providers review MCC's Program and report any Red Flags to the Program Administrator or MCC employee with primary oversight of the service provider relationship.

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 the Committee who developed this Program and 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 employees or the public. The Program Administrator shall inform the Committee and 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 shall be re-evaluated and updated periodically to reflect changes in risks to customers or the safety and soundness of MCC based on factors such as:

- 1) The experiences of MCC with identity theft;
- 2) Changes in methods of identity theft;
- 3) Changes in methods to detect, prevent, and mitigate identity theft;
- 4) Changes in the types of accounts that MCC offers or maintains;
- 5) Changes in the business arrangements of MCC, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

The reviews will include an assessment of which accounts are covered by the program, and the risk of identity theft with respect to each type of covered account.

Adopted and approved by the Metropolitan Community College Board of Governors 4/28/09