PROCEDURES FOR THE COLLEGE RED FLAGS RULE COMPLIANCE PROGRAM

I. Program Adoption

This program was adopted by the Board of Trustees for Monroe County Community College pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C.F.R. §681.2.

II. Program Purpose and Definitions

A. Fulfilling Requirements of the Red Flags Rule

This program is adopted to comply with the Red Flags Rule, which requires the establishment of an "Identity Theft Prevention Program" tailored to the size, complexity and nature of MCCC's operation.

B. Red Flags Rule Definitions Used in This Program

For purposes of this program, the following definitions apply:

1. Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.
2. Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.
3. Creditor: Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors.
4. Credit: The right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
5. Customer: Any current or former student, employee, or applicant for enrollment at MCCC.
6. Covered Account: A covered account includes:
   (a) Any account MCCC offers or maintains primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions; or
   (b) Any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of MCCC from Identity Theft.

7. Identifying Information: 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, unique electronic identification number, computer's internet protocol address, or routing code.
8. Service Provider: A third party that provides a service directly to MCCC.

III. Identification of Relevant Red Flags

Based on the types of covered accounts that MCCC offers and maintains, the methods it provides to open its covered accounts, the methods it provides to access its covered accounts, and its previous experiences with identity theft, MCCC identifies the following relevant red flags that may arise in connection with covered accounts and will train appropriate staff to recognize these red flags as they are encountered in the ordinary course of business:

A. Red Flags - Alerts, 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 a customer or applicant;
   3. Notice or report from a credit agency of an active duty alert for an applicant; and
   4. Notice or report from a credit agency of an address discrepancy.

B. Red Flags - 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 information on identification document that is not consistent with information provided by the person opening a new covered account, by the customer presenting the identification, or with existing customer information on file with the creditor (such as a signature card or recent check); and
   4. Application for service that appears to have been altered or forged.

C. Red Flags - Suspicious Personal Identifying Information
   1. Identifying Information presented that is inconsistent with other information the customer provides.
   2. Identifying Information presented is associated with common types of fraudulent activity, such as use of a fictitious billing address or phone number;

3. Identifying information presented that is consistent with known fraudulent activity, such as presentation of an invalid phone number or fictitious billing address used in previous fraudulent activity;
4. Social security number presented that is the same as one given by another customer;
5. An address or phone number presented that is the same as that of another customer;
6. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law, social security numbers must not be required); and
7. A person's identifying information is not consistent with the information that is on file for the customer.

D. Red Flags - Suspicious Account Activity or Unusual Use of Account
1. Change of address for an account followed by a request to change the account holder'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 (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the College that a customer is not receiving mail sent by the College;
6. Notice to the College that an account has unauthorized activity;
7. Breach in the College's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Red Flags - Alerts from Others
1. The College has received notice from a customer, identity theft victim, law enforcement or other person that the College has opened or is currently maintaining a fraudulent account.

IV. Detecting Red Flags

A. New Accounts
In order to attempt to detect any of the relevant red flags in connection with the opening of a new account, MCCC personnel will take the following steps, as may be appropriate under the circumstances, to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card); and
3. Independently contact the customer.

B. Existing Accounts
In order to attempt to detect any of the relevant red flags in connection with an existing account, MCCC personnel will take the following steps, as may be appropriate under the circumstances, to monitor transactions involving a covered account:

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. Responses to Red Flags

In the event MCCC personnel detect any relevant red flags, such personnel must contact the College's program administrator who will then decide which of the following steps should be taken:

1. Continue to monitor an account for evidence of identity theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify law enforcement; or
8. Determine that no response is warranted under the particular circumstances.

VI. Program Updates

MCCC will identify and appoint an appropriate individual to serve as program administrator. The program administrator will periodically review and update this program to reflect changes in risks from identity theft to customers or to the safety and soundness of MCCC. In doing so, the program administrator will consider MCCC's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the program administrator will determine whether changes to the program, including the identity of relevant red flags, are warranted. If warranted, the program administrator will update the program.

VII. Program Administration

A. Oversight

Responsibility for developing, implementing and updating this program lies with the program administrator. The program administrator will be responsible for the program's administration, for ensuring appropriate training of MCCC staff, for reviewing any staff reports (oral or written) regarding the detection of red flags and the responses to red flags, for determining which response should be taken in particular circumstances, and for considering periodic changes to the program.

B. Staff Training and Reports
All offices that may be responsible for implementing this program, including the Cashier's, Registrar's, Financial Aid, and Data Processing offices, will be trained in the detection of red flags and steps to be taken if a red flag is detected. The program will be reviewed periodically and revised, as needed.

C. 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 require the service provider(s) to verify that they are in compliance with all red flag requirements.

VIII. Duties Regarding Address Discrepancies

MCCC employees who use credit reporting information shall implement policies and procedures designed to enable the employees to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the employee receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

MCCC employees may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the consumer;
2. Review of MCCC's records;
3. Verification of the address through third-party sources; or
4. Other reasonable means.

If an accurate address is confirmed, the MCCC employee may furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. MCCC establishes a continuing relationship with the customer; and
2. MCCC, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.