POLICY

Title: RED FLAG – IDENTITY THEFT PREVENTION PROGRAM	Code: B0203
Authority: Board Minutes, 4/28/09	Original Adoption: 4/28/09 Revised/Reviewed: 4/28/09 Effective: 4/29/09

BACKGROUND
The Federal Trade Commission's "Red Flags" Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act") *requires financial institutions and creditors to develop and implement a written Identity Theft Prevention Program* designed to detect, prevent, and mitigate identify theft in connection with "covered accounts." MATC is a creditor for purposes of the FACT Act. After consideration of the size of the MATC's operations and account systems, and the nature and scope of MATC's activities, MATC developed this Identity Theft Prevention Program ("Program").

THE PURPOSE
The Program shall:

1. Identify relevant Red Flags for Covered Accounts;

2. Detect Red Flags in connection with opening of Covered Accounts and existing Covered Accounts;

3. Respond appropriately to any detected Red Flags including the reasonable mitigation of Identity Theft; and

4. Ensure that the Program is updated periodically to reflect changes in risks to students and to the safety and soundness of MATC.

As appropriate, the Program shall incorporate existing policies and procedures that control reasonably foreseeable risks.

DEFINITIONS
The following definitions are included as part of this policy:

1. Identity Theft. Fraud committed or attempted using the Identifying Information of another person without authority.

2. Covered Account. An account that MATC offers or maintains, primarily for personal, family, or household purposes that involves multiple payments or transactions; and, any other account MATC offers or maintains for which there is reasonably foreseeable risk to customers or to the safety and soundness of MATC from Identity Theft.

3. Red Flag. A pattern, practice or specific activity that indicates the possible existence of Identity Theft.

4. 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, driver license, identification number, alien registration number, government passport, employer or taxpayer identification number, student identification number, computer's internet protocol address, or routing code.

PROGRAM SPECIFICS

The Program procedures shall include reasonable steps to do all of the following:

1. Identify MATC's Covered Accounts and relevant MATC service provider Covered Accounts, if any.

2. Identify and establish risk factors in identifying relevant Red Flags including:
   a. Types of Covered Accounts
   b. Methods provided to open Covered Accounts
   c. Methods used to access Covered Accounts
   d. MATC's previous history of Identity Theft

3. Identify specific Red Flags including:
   a. Notification and warnings from credit reporting agencies
   b. Suspicious documents
   c. Suspicious identifying information
   d. Suspicious account activity
   e. Alerts from others

4. Detect Red Flags in appropriate areas including:
   a. Student Enrollment
   b. Existing Covered Accounts
   c. Credit Report Requests

5. Take one or more of the following steps when a Red Flag is triggered:
   a. Deny access to the Covered Account until other information is available to eliminate the Red Flag
   b. Contact the student
   c. Change any passwords, security codes or other security devices that permit access to a covered account
   d. Notify law enforcement
   e. Determine no response is warranted under the particular circumstances.

OVERSIGHT

The President or the President's Designee will serve as the Program Administrator and is responsible for developing, implementing and updating the Program. The Program Administrator will be responsible for ensuring appropriate training of MATC 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.

MATC staff responsible for implementing the Program shall be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. MATC staff are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of MATC's failure to comply with this Program. At least annually, MATC 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 agreements, significant incidents involving identity theft and management's response, and recommendations for changes to the program.

Service Provider Arrangements In the event MATC engages a service provider to perform an activity in connection with one or more covered accounts, MATC will require that the service provider review and comply with this Program including reporting any Red Flags to the Program Administrator

Specific Program Elements and Confidentiality
For the effectiveness of this Identity Theft Prevention Program, knowledge about specific procedures may need to be limited to those employees with a need to know. 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 contains are considered "confidential" and should not be shared with other MATC employees or the public. The Program Administrator shall inform the employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.