POLICY – Board of Trustees Montgomery College **76003**

Chapter: Administrative and Fiscal Services Modification No. 001

Subject: **Identity Theft Prevention Program**

I. The Federal Trade Commission's Red Flags Rule, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003, requires financial institutions and creditors to establish a policy to implement a written Identity Theft Prevention Program.

II. The Board of Trustees recognizes that some activities of the College are subject to the provisions of the Fair and Accurate Credit Transactions Act and the Red Flags Rule. Accordingly, to the extent the Red Flags Rule may apply, the College hereby establishes an Identity Theft Program to detect, identify, and mitigate theft in its covered accounts.

III. The president will implement an Identity Theft Program and procedures, as appropriate and as required by law

_____

Board Approval: January 25, 2013

PROCEDURE – Montgomery College **76003CP**

Chapter: Administrative and Fiscal Services Modification No. 001

Subject: **Identity Theft Prevention Program**

Montgomery College has developed this Identity Theft Prevention Program (Program) pursuant to the Federal Trade Commission's (FTC) Red Flags Rule. This Program formalizes and expands the College's existing policies, procedures, and practices to detect, prevent, and mitigate identity theft at the College in connection with the opening and operation of Covered Accounts as defined below. This Program addresses the size and complexity of the College's operations and account systems, as well as the nature and scope of the College's activities. Oversight for this program is the responsibility of the senior vice president for administrative and fiscal services.

I. Definitions

A. Identity Theft: fraud committed using the identifying information of another person.

B. Red Flags: a pattern, practice, or specific activity that indicates the possible existence of identity theft.

C. Account: a continuing relationship established by a person with the College to obtain a product or service for personal, household, or business purposes, including the extension of credit or deferring of payment.

D. Covered Account:

1. Any account that the College offers or maintains that is used primarily for personal, family, or household purposes and that involves or is designed to permit multiple payments or transactions; or

2. Any other account that the College offers or maintains for which there is a reasonably foreseeable risk to students or to the safety and soundness of the College from identity theft, including financial, operational, compliance, reputation, or litigation risks.

II. Covered Accounts

The College has identified the following types of Covered Accounts:

A. Federal Perkins loans

B. Installment tuition plans

C. Emergency student loans

All departments and offices with access to personally identifiable information relating to Covered Accounts are subject to this Program. Such departments and offices include, without limitation, the Offices of Enrollment Services and Financial Aid, Business Services, and Information Technology, regardless of where these departments and offices are located.

III. Identifying Red Flags

In order to identify relevant Red Flags, the College has considered the types of Covered Accounts that it offers and maintains, the methods it provides to open its Covered Accounts, the methods it provides to access its Covered Accounts, and its previous experience with identity theft. The College has identified the following Red Flags from each of the categories listed in the Red Flags Rule:

A. Suspicious Documents

The College collects or reviews documents from students in connection with various activities and transactions. For example, the College collects documents in connection with: requests for changes in name or address and applications for Perkins Loans, installment tuition plans, and emergency student loans (including the resolution of Caution Flags (or C-Flags) from the US government based on discrepant or insufficient information in federal student financial aid applications). This Program incorporates the following Red Flags relating to the presentation of suspicious documents:

1. An identification document or card appears to have been altered, forged, destroyed, or otherwise bears indicia of inauthenticity;

2. An identification document or card's physical description or photographic depiction appears inconsistent with the person presenting it;

3. Information on a document is inconsistent with other information provided by the person;

4. Information on a document is inconsistent with readily accessible information (for example, addresses of students) in the College's systems such as BannerWeb; and

5. An application or other request relating to a covered account appears to have been altered or forged.

B. Suspicious Personal Identifying Information

The College requires students to verify their identities for transactions related to Covered Accounts. Under this Program, Red Flags of suspicious personal identifying information include the following:

1. Identifying information that is inconsistent with other information the person provides (for example, inconsistent birth dates);

2. Identifying information that is inconsistent with other sources of information (for instance, an address not matching an address in the College's systems);

3. Identifying information, including a mailing address, e-mail address, phone number, or Social Security Number, that is identical to another person's information in the College's systems;

4. Identifying information matches information from applications or other materials that are known to be fraudulent or consistent with fraudulent activity (such as a known invalid phone number or known fictitious mailing address); or

5. In cases in which the College requires certain personal identifying information and requests such information from that person, the person fails to provide complete personal identifying information.

C. Unusual Use of, or Suspicious Activity Related to, a Covered Account

The College offers or maintains the Covered Accounts as defined in Section I.D. above. This Program considers the following Red Flags relating to the unusual use of, or suspicious activity related to, such Covered Accounts:

1. Shortly before a loan disbursement, loan refund disbursement, or transfer of funds to a student relating to a Covered Account, the College receives:

   a. a request related to such disbursement or transfer from an e-mail address other than the student's official Montgomery College e-mail address;

   b. a change of address request, especially when accompanied by other requests to change account information (such as a new telephone number or the addition of a new authorized user)**;** or

   c. a change in bank account information for electronic transfers.

2. The College learns that a student has not received a scheduled loan disbursement, loan refund disbursement or other transfer of funds.

3. Loan payments from a student cease on an otherwise consistently up-to-date Covered Account.

4. Correctly addressed mail or e-mail is repeatedly returned as undeliverable or the College otherwise learns that a student is not receiving mail or other communications from the College.

5. Suspicious activity (such as repeated unsuccessful login attempts) in connection with an online student account.

6. A breach of the College's computer system security affecting Covered Accounts.

7. Unauthorized access to or use of student account information relating to a Covered Account.

8. The College receives notice from a student, law enforcement officer, or other person of unauthorized activities in connection with a Covered Account.

D. Alerts from Others Regarding Possible Identity Theft in Connection with Covered Accounts

A Notice to the College from a student, victim of identity theft, law enforcement officer, or other person, that the College has opened or is maintaining a fraudulent account for a person engaged in identity theft is considered a Red Flag under this program.

IV. Detecting Red Flags

The College will use the measures set forth below to detect Red Flags. In addition, the College finds that its existing policies, procedures, and practices, which are incorporated into this Program—including, without limitation, Employee Responsibilities (Policy 31102); Confidentiality: Employee Use, Release and Disclosure of Information (Policy 31103); Student Cumulative Records (Policy 41003, which addresses requirements under the Family Educational Rights and Privacy Act); Acceptable Use of Information Technology Resources (Policy 76001); IT Program Network and Information Security and Privacy Program (Nov. 30, 2009, as amended); Confidential Data Management and Security (Policy 76002), and the Student Financial Aid Verification and File Review Policies and associated procedures—facilitate the detection of Red Flags and mitigate the risk of identity theft.

To detect Red Flags, the College will conduct the following activities related to the opening or maintenance of Covered Accounts.

A. Opening of Covered Accounts

1. The College will require applicants for Covered Accounts to authenticate their identity by providing, for example, name, date of birth, academic records, home address, Social Security Number, or other information.

2. The College will verify information provided by an applicant by reviewing documents presented that may include the applicant's driver's license, passport or other government-issued photo identification, birth certificate, social security card, certificate of naturalization, tax returns or other documents.

3. For Perkins loans, the College will follow federal law relating to the verification of applications and resolving conflicting information.

B. Existing Covered Accounts

1. The College will reasonably require photo-identification for any transaction involving a Covered Account and the presentation of correct identifying information for telephone transactions.

2. The College will require the use of an ID and password for any online transactions involving a Covered Account. The College's general authentication policies apply, for example:

a. authentication must occur before an individual may access any non-public College system or application;

b. User IDs must be unique;

c. A user must use his or her unique User ID and masked passwords of at least eight characters containing at least two valid password character attributes;

d. The College may not retrieve forgotten passwords. Reasonable methods are used to identify and authenticate the identity of a user prior to creating or allowing the creation of a new password (for example, correct responses to security questions).

3. The Office of Business Services authorizes transmission of funds to students. The Office of Business Services will authorize the transmission of funds relating to Covered Accounts only to:

a. the student after presentation of a government-issued photographic identification; or

b. the student's mailing address listed in the student's official file maintained by the Office of Enrollment Services and Financial Aid;

4. All students are assigned a College e-mail address that is used for the College's delivery of official e-mail communications.

V. Preventing and Mitigating Identity Theft

A. Immediate and Up-the-Ladder Reporting

Should any employee identify a Red Flag, he or she should *immediately* bring it to the attention of the employee's immediate supervisor and the senior vice president for administrative and fiscal services, and shall notify at least one of the following:

1. Vice President of Finance/Chief Financial Officer,

2. Chief Enrollment Services and Financial Aid Officer,

3. Director, Accounts Receivable and Treasurer, or

4. Director of Information Technology Policy and Administration.

B. Response

The Program Administrator or his or her designee will investigate the incident to determine whether identity theft or attempted identity theft has occurred or is likely to have occurred. The Program Administrator or designee will respond appropriately under the circumstances, which may include, without limitation:

1. Notifying the affected individual;

2. Monitoring the Covered Account for suspicious activity;

3. Contacting the account holder to verify activity in the Covered Account;

4. Changing passwords, security codes, or other security devices that permit access to the Covered Account;

5. Closing the Covered Account;

6. Notifying law enforcement; or

7. Determining that no response is warranted under the circumstances.

VI. Oversight of Service Providers

A. The College may use certain third party servicers, including an electronic commerce provider, to facilitate online course payments and refunds, and collection agents, in connection with Covered Accounts. The College will act to assure that service providers, conduct their activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Such measures may include:

1. Limiting the information shared with service providers;

2. Review of the service providers' identity theft prevention policies and practices; and/or

3. Requiring contractual representations relating to the service providers' identity theft prevention policies and practices, including without limitation:

a. Requiring service providers to have reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft;

b. Requiring service providers to comply with this Program.

VII. Program Administration

A. Oversight of the Program

The Program Administrator for this program is the senior vice president for administrative and fiscal services. However, the president may at any time designate a new Program Administrator from among senior management. The Program Administrator will be responsible for ensuring appropriate training of the College staff on the Program, reviewing any staff reports regarding the detection of Red Flags, determining the appropriate response to Red Flags to prevent and mitigate identity theft under the circumstances, implementing policies to further operationalize the Program, and evaluating periodic changes to the Program.

B. Staff Training and Reporting

College employees responsible for implementing the Program, including, but not limited to, the employees of the Offices of Business Services, Enrollment Services and Financial Aid, and Information Technology shall complete training in the detection of Red Flags and how to respond when a Red Flag is detected. Other

College employees shall be trained as appropriate to implement the Program effectively.
At least annually or as otherwise requested by the Program Administrator, the offices responsible for implementing the Program shall certify to the Program Administrator compliance with this Program. The report should address such issues as effectiveness of the Program 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 the College's response, and any recommendations for changes to the Program.

C. Program Updates

Annually, the Program Administrator will review this Program and, if necessary, update it to reflect changes in risks to students and to the College from identity theft. Such updates may include all aspects of the Program, including the list of Red Flags.

In so doing, the Program Administrator shall consider:

1. The College's experience with identity theft;

2. Changes in the methods of identity theft and its detection and prevention;

3. The addition of or changes to Covered Accounts;

4. The College's business arrangements with other entities;

5. Changes in the College's methods for identifying, detecting, and responding to Red Flags; and/or

6. Changes to technology utilized for cover accounts.

_____
Administrative Approval: January 25, 2013