

# MARSHALL UNIVERSITY BOARD OF GOVERNORS

## Policy No. FA-12

### IDENTITY THEFT PREVENTION PROGRAM

#### 1 General Information.

- 1.1 Scope: To identify, detect, and respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft.
- 1.2 Authority: W. Va. Code §18B-1-6
- 1.3 Passage Date: April 30, 2009
- 1.4 Effective Date: May 1, 2009
- 1.5 Statutory References: Fair and Accurate Credit Transactions Act of 2003, Section 114 and Federal Trade Commission's Red Flags Rule
- 1.6 History:
  - 1.6.1 This policy complements but does not amend or replace other information security procedures.

#### 2 Definitions and Program

##### 2.1 Red Flags Rule Definitions Used in this Program

- 2.1.1 "Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."
- 2.1.2 A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."
- 2.1.3 A "Covered Account" includes all student accounts or loans that are administered by the University.
- 2.1.4 "Program Administrator" is the individual designated with primary responsibility for oversight of the program. See Section VI below.
- 2.1.5 "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 code.

##### 2.2 Fulfilling Requirements of the Red Flags Rule

- 2.2.1 Under the Red Flags Rule, the University 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:
  - 2.2.1.1 Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
  - 2.2.1.2 Detect Red Flags that have been incorporated into the Program;

- 2.2.1.3 Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- 2.2.1.4 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

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

#### 3.1.1 Notifications and Warnings from Credit Reporting Agencies -- Red Flags

- 3.1.1.1 Report of fraud accompanying a credit report;
- 3.1.1.2 Notice or report from a credit agency of a credit freeze on an applicant;
- 3.1.1.3 Notice or report from a credit agency of an active duty alert for an applicant;
- 3.1.1.4 Receipt of a notice of address discrepancy in response to a credit report request; and
- 3.1.1.5 Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

#### 3.1.2 Suspicious Documents -- Red Flags

- 3.1.2.1 Identification document or card that appears to be forged, altered or inauthentic;
- 3.1.2.2 Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- 3.1.2.3 Other document with information that is not consistent with existing student information; and
- 3.1.2.4 Application for service that appears to have been altered or forged.

#### 3.1.3 Suspicious Personal Identifying Information -- Red Flags

- 3.1.3.1 Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
- 3.1.3.2 Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
- 3.1.3.3 Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- 3.1.3.4 Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- 3.1.3.5 Social security number presented that is the same as one given by another student;
- 3.1.3.6 An address or phone number presented that is the same as that of another person;
- 3.1.3.7 A person fails to provide complete personal identifying information on an application when reminded to do so; and
- 3.1.3.8 A person's identifying information is not consistent with the information that is on file for the student.

- 3.1.4 Suspicious Covered Account Activity or Unusual Use of Account -- Red Flags
  - 3.1.4.1 Change of address for an account followed by a request to change the student's name;
  - 3.1.4.2 Payments stop on an otherwise consistently up-to-date account;
  - 3.1.4.3 Account used in a way that is not consistent with prior use;
  - 3.1.4.4 Mail sent to the student is repeatedly returned as undeliverable;
  - 3.1.4.5 Notice to the University that a student is not receiving mail sent by the University;
  - 3.1.4.6 Notice to the University that an account has unauthorized activity;
  - 3.1.4.7 Breach in the University's computer system security; and
  - 3.1.4.8 Unauthorized access to or use of student account information.
- 3.1.5 Alerts from Others -- Red Flag
  - 3.1.5.1 Notice to the University from a student, Identity Theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

#### 4 Detecting Red Flags

##### 4.1 Student Enrollment

- 4.1.1 In order to detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account:
  - 4.1.1.1 Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
  - 4.1.1.2 Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

##### 4.2 Existing Accounts

- 4.2.1 In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:
  - 4.2.1.1 Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
  - 4.2.1.2 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; and
  - 4.2.1.3 Verify changes in banking information given for billing and payment purposes.

##### 4.3 Consumer ("Credit") Report Requests

- 4.3.1 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, University personnel will take the following steps to assist in identifying address discrepancies:
  - 4.3.1.1 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

- 4.3.1.2 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 University has reasonably confirmed is accurate.

## 5 Preventing and Mitigating Identity Theft

### 5.1 Prevent and Mitigate

- 5.1.1 In the event University 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:
  - 5.1.1.1 Continue to monitor a Covered Account for evidence of Identity Theft;
  - 5.1.1.2 Contact the student or applicant (for which a credit report was run);
  - 5.1.1.3 Change any passwords or other security devices that permit access to Covered Accounts;
  - 5.1.1.4 Not open a new Covered Account;
  - 5.1.1.5 Provide the student with a new student identification number;
  - 5.1.1.6 Notify the Program Administrator for determination of the appropriate step(s) to take;
  - 5.1.1.7 Notify law enforcement;
  - 5.1.1.8 File or assist in filing a Suspicious Activities Report (“SAR”); or
  - 5.1.1.9 Determine that no response is warranted under the particular circumstances.

### 5.2 Protect Student Identifying Information

- 5.2.1 In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University will take the following steps with respect to its internal operating procedures to protect student identifying information:
  - 5.2.1.1 Ensure that its website is secure or provide clear notice that the website is not secure;
  - 5.2.1.2 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;
  - 5.2.1.3 Ensure that office computers with access to Covered Account information are password protected;
  - 5.2.1.4 Avoid use of social security numbers;
  - 5.2.1.5 Ensure computer virus protection is up to date; and
  - 5.2.1.6 Require and keep only the kinds of student information that are necessary for University purposes.

## 6 Program Administration

### 6.1 Oversight

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

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

## 6.2 Staff Training and Reports

6.2.1 University 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. University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, University 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.

## 6.3 Service Provider Arrangements

6.3.1 In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University 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.

6.3.1.1 Require, by contract, that service providers have such policies and procedures in place; and

6.3.1.2 Require, by contract, that service providers review the University's Program and report any Red Flags to the Program Administrator or the University employee with primary oversight of the service provider relationship.

## 6.4 Non-disclosure of Specific Practices

6.4.1 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 University 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.

## 6.5 Program Updates

6.5.1 The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the University from Identity Theft. In doing so, the Committee will consider the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.