

MARYVILLE UNIVERSITY
IDENTITY THEFT PREVENTION PROGRAM

Effective Beginning August 1, 2009

I. PROGRAM ADOPTION

Maryville University (“University”) developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission’s (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This program was developed with approval of the Maryville University Board of Trustees. After consideration of the size and complexity of the University’s operations and account systems, and the nature and scope of the University’s activities, the Maryville University Board of Trustees determined that this Program was appropriate for the University, and therefore approved this Program on May 8, 2009. The categories, policies and procedures developed by the Program Administrator pursuant to this Program, as referenced herein, as specifically incorporated into the Program.

II. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program

“Identity Theft” is a “fraud committed or attempted using the identifying information of another person without authority.”

A “Red Flag” is a “pattern, practice, or special activity that indicates the possible existence of Identity Theft.”

A “Covered Account” includes all student accounts or loans that are administered by the University. It also includes staff accounts for which staff members make deferred payments for purchases.

“Program Administrator” is the individual designated with primary responsibility for oversight of the program. See Section VI below.

“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.

B. Fulfilling Requirements of the Red Flags Rule

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:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

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.

III. **IDENTIFICATION OF RED FLAGS**

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. With these items in mind, the University, through its Program Administrator, shall identify Red Flags in each of the listed categories prior to August 1, 2009:

- A. **Notifications and Warnings from Credit Reporting Agencies**
- B. **Suspicious Documents**
- C. **Suspicious Personal Identifying Information**
- D. **Suspicious Covered Account Activity or Unusual Use of Account**
- E. **Alerts from Others**

IV. **DETECTED RED FLAGS**

The University, through its Program Administrator, shall develop procedures for obtaining and verifying information regarding the following categories prior to August 1, 2009:

- A. **Student Enrollment**
- B. **Existing Accounts**
- C. **Consumer (“Credit”) Report Requests**

V. **PREVENTING AND MITIGATING IDENTITY THEFT**

The University, through its Program Administrator, shall develop steps that the University may take in the event University personnel detect any identified Red Flags. The University, through its Program Administrator, shall also develop steps that the University will take with respect to its internal operating procedures to protect student identifying information. Both of these actions shall be taken prior to August 1, 2009.

VI. **PROGRAM ADMINISTRATION**

A. **Oversight**

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 will be the Vice President for Administration and Finance. 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.

B. Staff Training and Reports

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.

C. Service Provider Arrangements

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.

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

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 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.

E. Program Updates

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 no less than annual. 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.