

# ADRIAN COLLEGE IDENTITY THEFT POLICY

## Adrian College's Identity Theft Prevention Program

### I. Program Adoption

The Vice President of Business Affairs has 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. After consideration of the size and complexity of Adrian College's operations and account systems, and the nature and scope of Adrian College's activities, Adrian College's Vice President of Business Affairs determined that this Program was appropriate for Adrian College, and therefore approved this Program on May 25, 2010.

### II. Definitions

"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 specific activity that indicates the possible existence of Identity Theft."

A "Covered Account" includes all student and employee accounts that are administered by Adrian College.

"Program Administrator" is the individual designated with primary responsibility for oversight of the program. See Section VII below.

### III. Covered Accounts

Adrian College has identified various types of accounts that fall within the definition of a covered account as set forth below:

1. Federal Perkins Loan Program
2. Student Accounts
3. Employee Benefit Accounts

#### **IV. Identification of Relevant Red Flags for Identity Theft**

Adrian College considers the following risk factors in identifying relevant red flags for identity theft for covered accounts:

1. Receipt of Notice of Dispute from a credit agency;
2. Identification document or card that appears to be forged, altered or inauthentic;
3. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
4. Other document with information that is not consistent with employee or student information;
5. Identifying information presented that is inconsistent with other information the employee or student provides (example: inconsistent birth dates);
6. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a Perkins loan application);
7. Social security number presented that is the same as one given by another student or employee;
8. Notice to Adrian College that an account has unauthorized activity;
9. Notice by student to Adrian College of unauthorized access to, or use of, student account information;
10. Notice to Adrian College from a student, employee, identity theft victim, law enforcement or other person that Adrian College has opened, or is maintaining, a fraudulent account for a person engaged in Identity Theft;
11. Student or employee signs a different name on registration or other forms;
12. Student or employee presents conflicting demographic information during registration without presenting a corroborating piece of identification;
13. Student receives a bill and asserts that he/she did not register for courses, housing, and/or meal plan at Adrian College and other processes indicate that this is likely to be true;
14. Student, student's representative or legal guardian, or employee admits during any process that someone else's identity is being used.

## **V. Detecting Red Flags of Identity Theft**

### **A. Student Enrollment**

In order to detect any of the Red Flags identified above associated with the enrollment of a student, Adrian College personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
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).

### **B. Existing Accounts**

In order to detect any of the Red Flags identified above for an existing Covered Account, Adrian College personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email).

### **C. Consumer Report Requests**

In order to detect any of the Red Flags identified above for an employment position for which a credit or background report is sought, Adrian College personnel will take the following steps to assist in identifying address discrepancies:

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.

## **VI. Preventing and Mitigating Identity Theft**

In the event Adrian College 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:

Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft;

2. Change any password or other security devices that permit access to Covered Accounts;
3. Notify the Program Administrator for determination of the appropriate step(s) to take;
4. Notify law enforcement;
5. Determine that no response is warranted under the particular circumstances.

#### Protect Student Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, Adrian College will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure; and
2. Ensure that system access to Covered Account information is password protected.

## **VII. Program Administration**

### **A. Oversight**

Responsibility for developing, implementing and updating the Program lies with an Identity Theft Committee (“Committee”) for Adrian College. The Committee is headed by a Program Administrator who is Adrian College’s Assistant Vice President of Business Affairs. The Program Administrator will be responsible for ensuring appropriate training of Adrian College 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**

Adrian College 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 responsible steps to be taken when a Red Flag is detected.

### **C. Program Updates**

The Committee will review and update this Program at least annually to reflect changes in risks to students, patients and employees and the soundness of Adrian College from Identity Theft. In

doing so, the Committee will consider Adrian College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in Adrian College'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 Program Administrator shall update the Program.

#### **D. Oversight of Service Provider Arrangements**

Adrian College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedure designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

### **VIII. Revision History**

Version: 1.0

Approved Date: May 25, 2010

Effective Date: June 1, 2010