SUBJECT: IDENTITY THEFT RED FLAGS POLICY

The Board of Trustees approves and adopts the Identity Theft Red Flags Policy dated April 23, 2009 stated below.

Central Michigan University Identity Theft Red Flags Policy and Procedures

Background

Central Michigan University ("CMU") has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This program was developed with oversight of the CMU Red Flag Committee and approval of the CMU Board of Trustees. After consideration of the size of CMU's operations and account systems, and the nature and scope of CMU's activities, the Board of Trustees determined that this Program was appropriate for CMU, and therefore approved this Program on April 23, 2009.

Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a "covered account" or an existing "covered account" (defined below) and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts CMU offers or maintains 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, staff, and faculty and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing CMU policies and procedures that control reasonably foreseeable risks.

Definitions

1. **Identify theft** means fraud committed or attempted using the identifying information of another person without authority

SUBJECT: IDENTITY THEFT RED FLAGS POLICY

2. **Sensitive information** means any information contained in a covered account that, if obtained, could lead to the commission of identity theft. Examples of sensitive information are listed below.

3. A **covered account** means: an account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Types of covered accounts at CMU are listed below.

4. A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Policy

CMU has identified numerous types of accounts containing sensitive information, which are covered accounts administered by the College. There are also six types of accounts that are administered by a third-party service provider.

College covered accounts include, but are not limited to:

1. Admissions
2. CMU Police (parking)
3. University Recreation
4. Educational Materials Center
5. Central Mailroom
6. Athletics
7. Beaver Island
8. Bookstore
9. Carls Center
10. Central Box Office and University Events
11. Development
12. Gay and Lesbian Programs
13. Graduate Studies
14. Human Environmental Studies (HEV)
15. Honors Program
16. Human Development Clinic (Counseling and Special Education)
17. Human Growth & Development Lab (HEV)
18. Information Technology (IT)
19. Office of International Education
20. Public Broadcasting
21. Public Relations and Marketing

SUBJECT: IDENTITY THEFT RED FLAGS POLICY

22. Receivable Accounting
23. Residence Halls
24. Recreation, Parks, and Leisure Services Administration
25. Sport Camps (Athletics)
25. Student Publications (CM Life)
26. Teacher Education and Professional Development

Service provider covered accounts include, but are not limited to:

1. Undergraduate Academic Services (UAS)
2. Money Network (Meta Bank)
3. General Revenue Corporation (GRC)
4. Recovery Management Services
5. American Collection Systems
6. Nelnet Business Solutions

Sensitive information includes the following items whether stored in electronic or printed format:

1. Credit card information, including any of the following:
   a. Credit card number (in part or whole)
   b. Credit card expiration date
   c. Cardholder name
   d. Cardholder address
2. Tax identification numbers, including:
   a. Social Security number
   b. Business identification number
   c. Employer identification numbers
3. Payroll information, including, among other information:
   a. Paychecks
   b. Pay stubs
   c. CMU Money Card
4. Cafeteria plan check requests and associated paperwork
5. Medical information for any employee or customer, including but not limited to:
   a. Doctor names and claims
   b. Insurance claims
   c. Prescriptions
   d. Any related personal medical information

SUBJECT: IDENTITY THEFT RED FLAGS POLICY

6. Other personal information belonging to any student, faculty, or staff member, examples of which include:
   a. Date of birth
   b. Address
   c. Phone numbers
   d. Maiden name
   e. Names
   f. Customer number

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above;

2. The methods provided to open covered accounts-- acceptance to CMU and enrollment in classes requires the following information:
   a. Common application with personally identifying information
   b. High school transcript
   c. Official ACT or SAT scores
   d. Entrance Medical Record
   e. Medical history
   f. Immunization history
   g. Insurance card

3. The methods provided to access covered accounts:

4. CMU's previous history, if any, of identity theft.

The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request made from a non-CMU issued E-mail account;
4. A request to mail something to an address not listed on file;
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts;

SUBJECT: IDENTITY THEFT RED FLAGS POLICY

6. Alerts, notifications, or warnings from a credit reporting or monitoring agency.

The above factors are not exhaustive; other factors can be considered in identifying red flags.

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement (if appropriate);
5. Determine no response is warranted under the particular circumstances.

Procedure

Responsibility for developing, implementing and updating this Program lies with the office of the Associate Vice President for Financial Services and Reporting. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of College's 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.

This Program will be reviewed at least yearly, and updated if necessary to reflect changes in risks to students and the soundness of CMU from identity theft. At least once per year, the Program Administrator will consider the College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the 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 will update the Program.

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 responsive steps to be taken when a Red Flag is detected.

The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures 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.