BOARD OF REGENTS

EASTERN MICHIGAN UNIVERSITY

SECTION: 22
DATE: April 17, 2012

RECOMMENDATION

REVISIONS TO RED FLAGS RULES POLICY

ACTION REQUESTED

It is recommended that the Board of Regents approve revisions to the University's Red Flags Rules policy.

STAFF SUMMARY

The revised policy, which was originally adopted in May 2009, has been changed to reflect the current responsibility for its implementation. The written procedures for the policy are also attached for your review.

FISCAL IMPLICATIONS

None

ADMINISTRATIVE RECOMMENDATION

The proposed Board action has been reviewed and is recommended for Board approval.

University Executive Officer **Date**

BOARD OF REGENTS
EASTERN MICHIGAN UNIVERSITY

Effective Date: May 1, 2009, Superseded April 17, 2012
Policy: Red Flags Rules

Formatted: Font color: Red

UNIVERSITY STATEMENT:

Eastern Michigan University is committed to preventing identity thieves from using someone else's identifying information to commit fraud. It is the policy of Eastern Michigan University to comply with the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Public Law 108-159. This amendment to the Fair Credit Reporting Act charged the Federal Trade Commission (FTC) with promulgating rules regarding identity theft. On November 7, 2007, the FTC promulgated the final rules, known as "Red Flags" rules, which have an effective date of December 31, 2010 ~~May 1, 2009~~.

To ensure compliance with the Red Flags rules, the Board of Regents authorizes the administration to develop and implement a written Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft.

Upon completion and presentation, the initial Identity Theft Prevention Program will be reviewed and approved by the Finance and Audit Committee of the Board of Regents.

The Red Flags rules are three different but related rules, two of which apply to Eastern Michigan University:

1. Users of consumer reports must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency.
2. Financial institutions and creditors holding "covered accounts" must develop and implement a written identitfy theft prevention program for both new and existing accounts.

Although the FTC, in many contexts, does not have jurisdiction over not-for-profit entities, it has taken the position that not-for-profits are subject to FTC jurisdiction when they engage in activities in which a for-profit entity would also engage. In its July 2008 guidance, the FTC stated "where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

UNIVERSITY PRACTICE:

University practices for implementing this policy include:

1. The development and enforcement of guidelines and procedures for an identity theft prevention program after consideration of the size and complexity of the University's operations and account system, as well as the nature and scope of the University's activities.

2. Train staff, as necessary to implement the program effectively.
3. Exercise appropriate and effective oversight of service provider arrangements.

RESPONSIBILITY FOR IMPLEMENTATION:

The President shall delegate to the Chief Financial Officer and the Provost and Vice President ~~of Student Affairs and Enrollment Services~~ the responsibility to oversee, develop, implement and administer the Identity Theft Prevention Program.

SCOPE OF POLICY COVERAGE:

This policy applies to all relevant University personnel and only insofar as necessary to supplement other training programs.

Eastern Michigan University Identity Theft Prevention Program

Employees Covered

The Federal Trade Commission (FTC) and Federal banking agencies issued a regulation known as the Red Flags Rule, intended to reduce the risk of identity theft. Eastern Michigan University is required to comply with the Red Flags Rule. All staff with access to *identifying information* must be familiar with and comply with the rules.

Definitions

Consumer Reporting Agencies- are entities that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes.

Consumer Reports- any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

- Credit or insurance to be used primarily for personal, family, or household purposes;
- Employment purposes; or
- Any other purpose authorized under US Code: Title 13k, 1681b

Covered Accounts- an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account. Any account that the financial institution or creditor offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

- **Includes all student accounts or loans that are administered by the University.**

Creditor- any person, corporation, government or government subdivision or agency, trust, estate, partnership, cooperative, or association who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Customer- a person that has a covered account with a financial institution or creditor.

Identifying information - 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 (IP) address
- routing code

Eastern Michigan University Identity Theft Prevention Program

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

Notice of Address Discrepancy- a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681 c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

Program Administrator- is the individual designated with primary responsibility for oversight of the program.

Red Flag- a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Service Provider- a person that provides a service directly to the financial institution or creditor.

The **EMU Identity Theft Prevention Program** is to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The University is required to develop reasonable processes and procedures to:

1. Identify relevant Red Flags
2. Detect Red Flags
3. Respond appropriately to prevent and mitigate identity theft
4. Administer the program

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 accounts, methods it provides to access accounts, and its previous experiences with Identity Theft. The University identifies the following Red Flags in each of the listed categories:

Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report
2. Notice or report from a credit agency of a credit freeze on an applicant
3. Notice or report from a credit agency of an active duty alert for an applicant
4. Receipt of a notice of address discrepancy in response to a credit report request
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity

Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document
3. Other document with information that is not consistent with existing student information

4. Application for service that appears to have been altered or forged

Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates)
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. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address)
5. Social security number presented that is the same as one given by another student
6. An address or phone number presented that is the same as that of another person, and the individuals do not reside together or cohabitate
7. A person fails to provide complete personal identifying information on an application when reminded to do so
8. A person's identifying information is not consistent with the information that is on file for the student

Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the student's name without adequate or appropriate documentation
2. Payments stop on an otherwise consistently up-to-date account
3. Account used in a way that is not consistent with prior use
4. Mail sent to the student is repeatedly returned as undeliverable
5. Notice to the University that a student is not receiving mail sent by the University
6. Notice to the University that an account has unauthorized activity
7. Breach in the University's computer system security
8. Unauthorized access to or use of student account information

Alerts from Others

Red Flag

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

Detecting Red Flags

Student Enrollment

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:

Detect

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

Existing Accounts

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:

Detect

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email)
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
3. Verify changes in banking information given for billing and payment purposes

Consumer ("Credit") Report Requests

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:

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
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

Preventing and Mitigating Identity Theft

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:

Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft
2. Contact the student or applicant (for which a credit report was run)
3. Change any passwords or other security devices that permit access to Covered Accounts
4. Not open a new Covered Account
5. Notify the Program Administrator for determination of the appropriate step(s) to take
6. Notify law enforcement
7. Provide the student with a new student identification number, if necessary
8. File or assist in filing a Suspicious Activities Report
9. 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, the University will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure
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
3. Ensure that office computers with access to Covered Account information are password protected
4. Use of social security numbers in compliance with University policies
5. Ensure computer virus protection is up to date
6. Require and keep only the kinds of student information that are necessary for University purposes

Program Administration

Oversight

Responsibility for developing, implementing and administering this Program is jointly assigned to the University's Chief Financial Officer and the Provost.

Staff Training and Reports

University staff responsible for handling covered accounts and implementing the Program shall be trained 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 Director of Student Business Services once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program. At least annually there shall be a report on the compliance with this Program.

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

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 those employees with a need to know. Any documents produced in order to implement this program that list or describe specific practices and the information those documents contain may be classified "confidential" and not shared with other university employees or the public.

Additional Resources

Identity Theft Resource Center: http://www.idtheftcenter.org/

Federal Trade Commission – Fighting Back Against Identity Theft: http://www.ftc.gov/bcp/edu/microsites/idtheft/

U.S. Department of Education, Office of the Inspector General - Resource on Identity Theft for Students: http://www2.ed.gov/about/offices/list/oig/misused/idtheft.html

Michigan State University, Identity Theft Program: http://www1.cj.msu.edu/~outreach/identity/

U.S. Identity Theft Task Force: http://www.idtheft.gov/