Western Michigan University

Identity Theft Prevention

(also known as the "Red Flag rules")

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. Western 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.

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. By identifying Red Flags in advance, you will be better able to spot suspicious patterns when they arise and take the necessary steps to prevent them becoming an episode of Identity Theft.

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 (IP) address
- or routing code.

The 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) Identity relevant Red Flags

2) Detect Red Flags

3) Prevent and mitigate identity theft

4) Program Administration

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:

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

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; and
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; and
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; and

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; and

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

A. 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; 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, 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; and

3. Verify changes in banking information given for billing and payment purposes.

C. 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; and

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 ("SAR"); or

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 the University's Social Security Number Policy;

5. Ensure computer virus protection is up to date; and

6. Require and keep only the kinds of student information that are necessary for University purposes.

Program Administration

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the office of the Treasurer of the Board, the Vice President for Business and Finance.

B. 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 Accounting 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.

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 University employee with primary oversight of the service provider relationship.