



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: **CAMPUS: GENERAL MATTERS** Policy No. **CGM 0880**

Title: **Red Flag Rule – Protection of Student Identities**

Effective Date: **November 1, 2009**

Page No. 1 of 9

GENERAL PURPOSE:

This policy is intended to provide a process and procedure that will insure the uniform administration of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

GLOSSARY OF SIGNIFICANT TERMS USED:

Application: The paper work a person needs to complete in order to be considered for admission or readmission to MJJ.

Covered accounts: are described as an account that a creditor holds that is designed to allow multiple payments or transactions after services have been delivered.

Creditor: means any person who regularly extends, renews, or continues credit.

Identity theft: is defined as a “fraud committed or attempted using the identifying information of another person without authority”.

Red Flag: is defined as a pattern, practice or specific activity that indicates the possible existence of identity theft. Examples of “Red Flag” incidents include presentation of suspicious identity documents or frequent address changes.

Registration: What an admitted student does before any semester in which s/he desires to take classes. That is, the admitted student signs up for classes by **registering** for them. It has nothing to do with **applying** or **application**.

BACKGROUND/POLICY:

In late 2007 the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The regulation is intended to reduce the growing risk of identity theft by requiring stronger fraud prevention to protect consumers’ personal data.



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: CAMPUS: GENERAL MATTERS Policy No. CGM 0880

Title: Red Flag Rule – Protection of Student Identities

Effective Date: November 1, 2009

Page No. 2 of 9

Identity theft is defined as a “fraud committed or attempted using the identifying information of another person without authority”. An identity can be stolen with a few pieces of personal identifying information, obtained from a variety of sources, including misplaced documentation, stolen mail, computer hacking, fraudulent address changes and other nefarious schemes.

The Red Flag Rule applies to any organization that offers credit or manages a “covered account”, and requires the organization to establish, document, and maintain an identity theft prevention program that will identify potential Red Flags, detect the occurrence of Red Flags, and appropriately respond to Red Flags.

IMPLICATIONS FOR MJI

A “Red Flag” is defined as a pattern, practice or specific activity that indicates the possible existence of identity theft. Examples of “Red Flag” incidents include presentation of suspicious identity documents or frequent address changes.

“Covered accounts” are described as an account that a creditor holds that is designed to allow multiple payments or transactions after services have been delivered.

“Creditor” means any person who regularly extends, renews, or continues credit.

MJI is subject to Red Flag rules because we act as “creditors” holding covered accounts by participating in or offering:

- Student tuition and fee payment plans
- Federal Loan programs

MJI has developed and adopted this Identity Theft Prevention Program tailored to its size, complexity and nature of its operation which will help the college identify, detect and respond to red flags, and to continuously upgrade its environment to ensure best



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: CAMPUS: GENERAL MATTERS Policy No. CGM 0880

Title: Red Flag Rule – Protection of Student Identities

Effective Date: November 1, 2009

Page No. 3 of 9

practices in this regard.

The program contains 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.

PROCESS:

In order to identify relevant Red Flags, Michigan Jewish Institute (MJI) 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. MJI identifies the following Red Flags in each of the listed categories:

A. 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.

B. 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



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: CAMPUS: GENERAL MATTERS Policy No. CGM 0880

Title: Red Flag Rule – Protection of Student Identities

Effective Date: November 1, 2009

Page No. 4 of 9

- 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.

C. 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;
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.

D. 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;
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 MJI that a student is not receiving mail sent by MJI;
6. Notice to MJI that an account has unauthorized activity;
7. Breach in MJI's computer system security; and



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: **CAMPUS: GENERAL MATTERS** Policy No. **CGM 0880**

Title: **Red Flag Rule – Protection of Student Identities**

Effective Date: **November 1, 2009**

Page No. **5 of 9**

8. Unauthorized access to or use of student account information.

E. Alerts from Others Red Flag

1. Notice to MJI from a student, Identity Theft victim, law enforcement or other person that MJI has opened or is maintaining a fraudulent account for a person engaged in Identity Theft. 5

DETECTING RED FLAGS

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, MJI 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, MJI 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.



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: **CAMPUS: GENERAL MATTERS** Policy No. **CGM 0880**

Title: **Red Flag Rule – Protection of Student Identities**

Effective Date: **November 1, 2009**

Page No. **6 of 9**

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, MJI 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 MJI has reasonably confirmed is accurate.

PREVENTING AND MITIGATING IDENTITY THEFT

In the event MJI 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. Provide the student with a new student identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report (“SAR”); or



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: **CAMPUS: GENERAL MATTERS** Policy No. **CGM 0880**

Title: **Red Flag Rule – Protection of Student Identities**

Effective Date: **November 1, 2009**

Page No. 7 of 9

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, MJI 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. Avoid use of social security numbers (See Information Use 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 MJI purposes.

PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee ("Committee") for the MJI. The Committee is chaired by MJI's designated Security Officer (the name of the current Security Officer may be found in the current *Academic Catalog and Student Handbook* in the section on "Campus Security and Statistics). Two or more other individuals appointed by the President of MJI or the Dean of Academic Administration comprise the remainder of the committee membership, with at least one other member representing the MJI Office of Financial Aid. The Committee Chair will be responsible for ensuring appropriate training of MJI staff on this Red Flag policy, 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



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: CAMPUS: GENERAL MATTERS Policy No. CGM 0880

Title: Red Flag Rule – Protection of Student Identities

Effective Date: November 1, 2009

Page No. 8 of 9

circumstances and considering periodic changes to the Red Flag policy.

B. Staff Training and Reports

MJI staff responsible for implementing the Red Flag policy shall be trained either by or under the direction of the Committee Chair in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. MJI staff shall be trained, as necessary, to effectively implement the Policy. MJI employees are expected to notify the Committee Chair once they become aware of an incident of Identity Theft or of MJI's failure to comply with this Policy.

At least annually or as otherwise requested by the Committee Chair, MJI staff responsible for development, implementation, and administration of this Red Flag Policy shall report to the Committee Chair on compliance with this Red Flag Policy. 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 Red Flag Policy.

C. Service Provider Arrangements

In the event the MJI engages a service provider to perform an activity in connection with one or more Covered Accounts, MJI 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 MJI's Red Flag Policy and report any Red Flags to the Committee Chair or MJI employee with primary oversight of the service provider relationship.



MICHIGAN JEWISH INSTITUTE

Policy and Procedure Manual

Functional Area: **CAMPUS: GENERAL MATTERS** Policy No. **CGM 0880**

Title: **Red Flag Rule – Protection of Student Identities**

Effective Date: **November 1, 2009**

Page No. **9 of 9**

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 Red Flag Policy 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 policy that list or describe such specific practices and the information those documents contain are considered “confidential” and should not be shared with other employees or the public. The Committee Chair 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 Red Flag Policy to reflect changes in risks to students and the soundness of the MJI Identity Theft policy. In doing so, the Committee will consider MJI's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in MJI's business arrangements with other entities. After considering these factors, the Committee Chair will determine whether changes to the policy, including the listing of Red Flags, are warranted. If warranted, the Committee will update this policy.

AUTHORIZATIONS: (at least one signature is necessary to enact this policy/procedure)

President

Dean Of Academic Administration



This section reserved for any forms and addenda that may be created for this policy