UM Identity Theft Protection Policy

Summary/Purpose: The purpose of the UM Identify Theft Protection Policy is to establish an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flag Rules, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

UM recognizes that some activities of the university are subject to the provisions of the Fair and Accurate Credit Transactions Act (FACT Act) 16 CFR § 681. Per the Federal Trade Commission(FTC) definition, this activity could include participation in the Federal Perkins Loan or Federal Direct Loan programs, as well as institutional loans to faculty, staff, or students, and tuition payment plans. While UM may not participate in all these activities, the university strives to protect all personally Identifyable Information (as defined herein) and prevent identity theft, as required by the FTC Red Flag Rules.

1. Definitions

1.1. "Covered Accounts" means any account that a Creditor offers or maintains for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

1.2. "Creditor" means any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

1.3. "Identity Theft" means fraud committed or attempted using the identifying information of another person without authorization.

1.4. "Personally Identifiable Information" mean any piece of information, which may be used to uniquely identify, contact, or locate an individual, and includes, but is not limited to

(a) taxpayer identification numbers

(b) driver's license numbers

(c) passport identification numbers

(d) passwords

(e) personal identification numbers (PINs)

(f) personal account numbers

(g) computer accounts and passwords

(h) protected health information

(i) financial information

(j) unpublished home addresses or phone numbers, and

(k) any combination of information that will uniquely identify an individual.

1.5. "**Program Administrator"** means the UM bursar or other designated representative of the Vice Chancellor for Administration and Finance.

1.6. **"Red Flag"** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

2. General Policy

2.1 Included Procedures. As required by the Red Flag Rules, the Identity Theft Prevention Program ("Program") shall include procedures for:

(a) Identifying relevant red flags for new and existing covered accounts,

(b) Detecting red flags that have been incorporated into the Program, and

(c) Responding appropriately to detected red flags in order to prevent and mitigate identity theft.

2.2 Periodic Updates. The Program will be periodically updated to reflect environmental, institutional, and legal changes.

3. Authority and Responsibility

3.1 Responsibilities of the Program Administrator. The Program Administrator will exercise appropriate and effective Program oversight and will work with the department administrators in areas impacted by the Red Flag Rules. (See Appendix A for a list of these areas.) The Program Administrator is responsible for:

(a) Developing, implementing, assessing, and updating the Program;

(b) Developing and maintaining a training program;

(c) Ensuring compliance of university staff; and

(d) Reviewing any red flag detection reports and initiating the appropriate response actions.

3.1 Annual Assessment and Reporting. The Program Administrator shall conduct an annual Program assessment and provide a report to the Vice Chancellor for Finance and Administration, to include recommended Program changes.

3.2 Third Party Vendors. Third party vendors who process any payments for or on behalf of the university will be required to acknowledge their responsibilities under and to comply with the FTC's Red Flag Rules.

3.3 Responsibilities of All UM Personnel. In the event university personnel detect any identified red flags or related suspicious activity, such personnel shall report it immediately to the Program Administrator, who will conduct further investigation and initiate the appropriate response actions.

3.4 Departmental Specific Practices. Each department impacted by this Program shall have the authority to development internal procedures specific to their area, as appropriate, related to compliance with this Policy. Any such procedures shall be maintained interdepartmentally in writing and made available to the Program Administrator upon request.

3.5 Non-disclosure of Specific Practices. For the effectiveness of this Program, knowledge about specific Red Flag identification, detection, mitigation, and prevention practices may need to be limited to the Program Administrator or other designated employees.

4. Identification of Red Flags

After a comprehensive evaluation of the UM environment, the following items will be considered red flags:

(a) Notifications and Warnings from Credit Reporting Agencies

(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

(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 customer information (such as if a person's signature on a check appears forged); and

(4) An application for service that appears to have been altered or forged.

(c) Suspicious Personal Identifying Information

(1) Identifying information presented that is inconsistent with other information the customer 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 credit report),

(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 customer,

(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 (however, by law, social security numbers must not be required), and

(8) A person's identifying information is not consistent with the information that is on file for the customer.

(d) Suspicious Covered Account Activity or Unusual Use of Account

(1) Change of address for an account followed by a request to change the account holder'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 (example: very high activity),

(4) Mail sent to the account holder is repeatedly returned as undeliverable,

(5) Notice to the university that a customer is not receiving mail sent by the university,

(6) Notice to the university that an account has an unauthorized activity,

(7) Breach in the university's computer system security, and

(8) Unauthorized access to or use of the customer's account information.

(e) Alerts from Others. These shall include notice to the university from a faculty, staff, or student, identity theft victim, law enforcement, or other person regarding possible identity theft in connection with covered accounts.

5. Detecting Red Flags

In order to detect the red flags for a new or existing account, university personnel will verify:

(a) The identification of customers, if they request information (in person, via telephone, via facsimile, via email);

(b) The validity of requests to change billing addresses; and

(c) The accuracy of any banking information changes that impact billing and payment.

6. Consumer Credit Report Requests

In the event credit reports are required for employment or in the creation of other Covered Accounts, university personnel will take the following steps to detect red flags to identify address discrepancies:

(a) Require written address verification from any applicant at the time the request for the credit report is made to the consumer reporting agency, and

(b) Verify that the credit report pertains to the applicant for whom the requested report was made in the event of an address discrepancy. Personnel should notify the consumer- reporting agency and provide the relevant address information.

7. Response Actions

7.1 Actions upon Detection or Report of Red Flags. The Program Administrator will determine the appropriate response actions, if any, upon detection or report of red flags, in accordance with requirements of FACT Act and other applicable regulations. Such actions may include:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

7.2 Log of Red Flag Detections. The Program Administrator will log all reported red flag detections, along with the actions taken, to be included in the annual report for the Vice Chancellor for Administration and Finance.

Appendix A

University of Mississippi Departments That Must Comply With the Red Flag Rules

The following business areas and support units have been determined to fall under the requirements of the FTC Red Flag Rules or determined by UM administration to otherwise be affected by this policy and must appoint a representative to work with the Program Administrator:

- Alumni Affairs
- Bursar
- Campus Recreation
- Chemistry/Biochemistry
- Counseling Center
- Dean of Students
- Employee Health
- Golf Course/Landscaping Services
- Graduate School
- Health Promotion
- ID Center
- Intercollegiate Athletics
- Law School
- Outreach
- Parking and Transportation Services
- Pharmacy
- Physical Plant Department
- Procurement
- Registrar
- School of Education
- Speech and Hearing
- Student Health
- Student Health Pharmacy
- Student Housing
- Student Media Center
- Telecommunications
- University Publications
- University Police Department
- Willie Price Nursery

Other areas will be added as necessary.