THE UNIVERSITY OF MICHIGAN
REGENTS COMMUNICATION

ACTION REQUEST

Approved by the Regents
October 15, 2009

Subject: Identify Theft Prevention Program

Action Requested: Approval of Program

Background:

In the Fair and Accurate Credit Transactions Act of 2003 Congress required the Federal Trade Commission and other federal agencies to promulgate rules to protect against identify theft. The Federal Trade Commission promulgated applicable rules, commonly known as the Red Flag Rules, and adopted an effective date of January 1, 2008. Enforcement of the rules has been postponed many times and the current date for enforcement of the mandatory compliance is set for November 1, 2009. For an institution such as the University of Michigan, compliance requires adoption of policies regarding address discrepancies in credit reports and detecting and acting upon possible instances of identity theft for "covered accounts". In general, "covered accounts" are loans or other situations where a person obtains money, goods or services by presenting in part, appropriate proof of identity (and of course, meeting applicable qualifications for the item).

I recommend that the Regents approve the attached Identify Theft Prevention Program.

Respectfully submitted,

Timothy P. Slottow
Executive Vice President and
Chief Financial Officer

October 2009
Attachment

Identity Theft Prevention Program

I. Purpose & Scope

The Identity Theft Prevention Program was developed pursuant to the Federal Trade Commission's Red Flag Rules promulgated as part of the Fair and Accurate Credit Transactions Act. The University's Program is designed to detect, prevent and mitigate identify theft in connection with the opening of a covered account or any existing covered accounts within the University's Ann Arbor, Flint and Dearborn Campuses. The Program has been designed to be appropriate to the size and complexity of the University as a creditor and the nature and scope of its activities.

II. The "Red Flag Rules" Overview

The Red Flag Rules, found at 16 CFR § Part 681, require users of consumer credit reports, certain creditors and certain card issuers to take various steps to protect consumers from identity theft.

Users of credit reports must respond to notices of address discrepancies and take reasonable steps to confirm the accuracy of the address it may have.

A creditor must periodically determine, by conducting a risk assessment, whether it offers or maintains covered accounts. Upon identifying any covered account(s), the creditor is required to develop and implement a written Identity Theft Prevention Program designed to:

A. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
B. Detect Red Flags;
C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
D. Periodically update the program to reflect changes in risks to the account holders or to the safety and soundness of the creditor from Identity Theft.

A card issuer must establish and implement reasonable address verification procedures.

Oversight and administration of the Program shall be performed by the Office of the Chief Financial Officer in consultation with the Provost and the Chief Financial Officer for UM Health System. Periodic reports on the progress of program implementation will be provided to the Finance, Audit, and Investment Committee of the Board of Regents.

III. Definitions

A. **"Account"** means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. It includes (i) an extension of credit, such as the purchase of property or services involving a deferred payment, and (ii) a deposit account.

B. **"Covered Account"** means (i) 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 and (ii) any other account that the creditor offers to maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

C. **"Identity Theft"** means a fraud committed or attempted using the identifying information of another person without authority.

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

E. **"Service Provider"** means a person that provides a service directly to the financial institution or creditor.

IV. Covered Accounts Maintained by the University of Michigan

A. External Loan Programs
B. Internal Loan Programs
C. Student Accounts
D. Other accounts that may be identified by units as meeting the definition of Covered Account.

V. Identification of Red Flags

In identifying below specific Red Flags unique to these covered accounts and the applicable business procedures of the University, the University considered the following risk factors: the types of covered accounts offered and maintained, the methods provided for opening and accessing each of those accounts, prior experiences with Identity Theft, and the size, complexity, nature and scope of our institution and its activities. Each of the Red Flags mentioned below may only be applicable to certain of the covered accounts administered by the University.

1. Receipt of a notice of address discrepancy from a credit reporting agency;

2. Documents presented in an application or for the purpose of personal identification are incomplete or appear to have been altered, forged or inauthentic; or are inconsistent with the appearance of the individual presenting the document; or are inconsistent with readily accessible information on file with the University;

3. Challenge questions, used by University to allow students and individuals to access their covered accounts, are answered incorrectly; and

4. The University is notified of special problems in connection with a student's or individual's covered account such as unauthorized charges or transactions, lost or stolen University identification documents, a fraud alert or the account holder is a victim of identity theft.

5. Other red flag indicators that may be identified by the units for their specific covered accounts.

VI. Red Flag Response

After detection of a Red Flag identified above, the following actions will be taken by the University departments that maintain covered accounts under this program, when appropriate given the particular covered account at issue and under the particular circumstances, to confirm the identity of students and individuals when they open and/or access their covered accounts:

A. Obtain appropriate personal identifying information (e.g., photo identification, date of birth, academic status, user name and password, address, etc.) from the student or individual account holder, prior to issuing a new or replacement ID card, opening a covered account, or allowing access to a covered account.
B. Provide notification when certain changes to a covered account are made online, to students and individuals holding covered accounts to confirm the change was valid and to provide instruction in the event the change is invalid.
C. Verify suspicious changes made to covered accounts that relate to an account holder's identity, administration of the account, and billing and payment information.
D. Notify appropriate University personnel accessing records related to the affected account holder that a Red Flag has been detected.

VII. Prevention and Mitigation of Identity Theft

In addition to the efforts noted above to detect Identity Theft, University personnel involved in the administration of the covered accounts will take the following steps, where appropriate and based upon the particular circumstances, to prevent and mitigate occurrences of Identity Theft when a Red Flag is detected:

A. Monitor a covered account for evidence of Identity Theft;
B. Contact student(s) and/or individual account holder(s);
C. Request additional documentation from the student and/or individual account holder to verify identity;
D. Change passwords, security codes and other security devices permitting access to the covered account;
E. Reopen a covered account with a new account number;
F. Decline to open a new covered account;
G. Close an existing covered account;
H. Notify law enforcement;
I. Determine that no response is warranted under the particular circumstances;
J. Attempt to identify the cause and source of the Red Flag; and
K. Take appropriate steps to modify the applicable process to prevent similar activity in the future.
L. Notify appropriate University personnel accessing records related to the affected account holder that a Red Flag has been detected.

VIII. Program Administration

A. Administration and Oversight: Authority to implement and administer the Program and to approve future revisions to the Program shall be delegated to the Chief Financial Officer and the Associate Vice President for Finance.

B. Staff Training: University departments that maintain covered accounts should develop and implement plans to effectively train their staff in the identification, detection, prevention and mitigation of the Red Flags identified above that are unique to their specific covered accounts. Staff training should be conducted on a regular basis and as necessary under the circumstances related to the administration of the particular covered account.

C. Oversight of service providers: If and when the University engages a service provider to perform an activity in connection with a covered account, University departments that maintain covered accounts under this program should take steps necessary to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

D. Reporting: At least annually, University departments that maintain covered accounts under this program should report to the Office of the Chief Financial Officer,

regarding their compliance with this Program. The reporting should address the following elements:

- The department's identification of covered accounts is accurate and up to date, and the department has developed local policies and procedures for addressing the Red Flags associated with the related covered accounts.
- The department has conducted the appropriate training for their staff as necessary and has taken the appropriate steps to ensure any service provider activity is conducted appropriately.
- The department has reported significant Red Flag occurrences as appropriate.
- Suggested program updates or changes as applicable to the Department.

E. Program Assessment and Update: The Office of the Chief Financial Officer will periodically review and update the Program based on an assessment of the following factors: prior experiences with identity theft; changes in the methods of identity theft; changes in the method of detection, prevention and mitigation of identity theft; the covered accounts offered and administered by the University; and the potential Red Flags that may arise with respect to the Covered Accounts. This assessment will consider changes in risks to students and individual account holders of identity theft, findings from the annual departmental reports, and the safety and soundness of the University's identify protection systems.