

Doc. T08-109

Passed by the Board of Trustees

December 11, 2008

**UNIVERSITY OF MASSACHUSETTS
IDENTITY THEFT PREVENTION PROGRAM**

The Board recognizes that some activities of the University are subject to the provisions of the Fair and Accurate Credit Transactions Act (FACT Act) and its “Red Flag” rules.

Therefore, the Board of Trustees adopts the following initial program Identity Theft Prevention Program for the University of Massachusetts system.

I. Program Adoption

The University of Massachusetts has adopted this initial Identity Theft Prevention Program ("Program") in compliance with the “Red Flag” rules issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions ACT (“FACTA”). The University is engaging in activities which are covered by the FACTA Red Flag rules. After consideration of the size and complexity of the University’s operations and account systems, and the nature and scope of the University’s activities, the Board has determined that this Program is appropriate for the University.

II. Program Purpose

Under the Red Flag rules, the University is required to establish an “Identity Theft Program” with reasonable policies and procedures to detect, identify, and mitigate identity theft in its covered accounts. The University must incorporate relevant Red Flags into a Program to enable the University to detect and respond to potential identity theft. The University shall ensure that the Program is updated periodically to reflect changes in risks to customers or creditors or the University from identity theft.

III. Responsible University Official

The President shall designate a senior University official to serve as Program Administrator. The Program Administrator shall exercise appropriate and effective oversight over the Program and shall report regularly to the President on the Program.

IV. Program Administration and Maintenance

The Program Administrator is responsible for developing, implementing and updating the Program throughout the University system. The Program Administrator will be responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for identifying, preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

The Program will be periodically reviewed and updated to reflect changes in identity theft risks and technological changes. The Program Administrator will consider the University’s experiences with

identity theft, changes in identity theft methods; changes in identity theft detection, mitigation and prevention methods; changes in types of accounts the University maintains; changes in the University's business arrangements with other entities, and any changes in legal requirements in the area of identity theft. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted.

The Program Administrator shall confer with all appropriate University personnel as necessary to ensure compliance with the Program. The Program Administrator shall annually report to the President on the effectiveness of the Program. The Program Administrator shall present any recommended changes to the President for approval. The President's approval shall be sufficient to make changes to the University Identity Theft Program.

V. Definitions

Pursuant to the Red Flag regulations at 16 C. F. R. § 681.2, the following definitions shall apply to this Program:

Covered accounts:

1. Any account the University offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions.
2. Any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from Identity Theft.

Credit: The right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefor.

Creditor: An entity that regularly extends, renews, or continues credit.

Customer: Any person with a covered account with a 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
- unique electronic identification number
- computer's Internet Protocol address or routing code

Identity Theft: A fraud committed using the identifying information of another person.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

VI. Identification of Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The following are relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on a customer or applicant;
- Notice or report from a credit agency of an active duty alert for an applicant; and
- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- 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
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another customer;
- An address or phone number presented that is the same as that of another person;
- 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
- A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example: very high activity);
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to the University that a customer is not receiving mail sent by the University;
- Notice to the University that an account has unauthorized activity;
- Breach in the University's computer system security; and
- Unauthorized access to or use of customer account information.

E. Alerts from Others

- Notice to the University from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

VII. Detecting Red Flags

The Program's general Red Flag detection practices are described in this document. The Program Administrator and each campus will develop and implement specific methods and protocols appropriate to meet the requirements of this Program.

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
- Verify the customer's identity (for instance, review a driver's license or other identification card);
- Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, University personnel will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
- Verify the validity of requests to change billing addresses; and
- Verify changes in banking information given for billing and payment purposes.

VII. Responding to Red Flags and Mitigating Identity Theft

In the event University personnel detect any identified Red Flags, such personnel shall all appropriate steps to respond and mitigate identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:

- Continue to monitor an account for evidence of Identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;
- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

VIII. Staff Training and Reporting

University employees responsible for implementing the Program shall be trained under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

Appropriate staff shall provide reports to the Program Administrator on incidents of identity theft, the effectiveness of the Program and the University's compliance with the Program.

IX. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more 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 Utility's Program and report any Red Flags to the Program Administrator.