MIT Identity Theft Prevention Program for Covered Accounts under the FTC Red Flags Rule

I. INTRODUCTION AND OVERVIEW

MIT has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's 2007 "Red Flags Rule," 16 C. F. R. § 681.2, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. These regulations require "financial institutions" and "creditors" that hold "covered accounts" to "develop and implement an identity theft prevention program" for new and existing accounts. (See Section III for definitions.) The FTC regulations include a list of twenty-six "red flags" that might indicate the potential for identity theft. All creditors are required to review their processes, and identify applicable red flags – either from the FTC's list, or ones more appropriate to their situation. Creditors are then required to define the steps by which the red flags will be detected and their response once a red flag is detected.

Based on the definitions used in these regulations, there are several areas at MIT where this Program applies, including student loans, such as Perkins Loans, faculty housing loans, and educational loans to staff. This Program may also apply to any other business functions of MIT which allow individuals to defer payment for product or services.

In designing the Program, MIT is permitted to incorporate, as appropriate, its existing policies and procedures. In particular, this program is designed in the context of MIT's existing Information Policies as well as recommendations for the security of electronic data and systems.

II. PROGRAM ADOPTION

This Program was developed by a working group including members of the Office of the General Counsel, Audit Division, and Information Services & Technology, and in consultation with key business process owners, such as Student Financial Services and Faculty Housing.

After consideration of the size and complexity of MIT's operations and account systems, the nature and scope of MIT's activities, and the pattern and risks of identity theft, it was determined that this Program was appropriate for MIT.

The Program was approved by MIT's Audit Committee on April 22, 2009.

III. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flags Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity, and the nature of its operation. Each Program must contain 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 individuals or to the safety and soundness of MIT from identity theft.

B. Red Flags Rule definitions used in this Program

Account: a continuing relationship with a creditor to obtain a product or service that includes deferred payments for services or property.

Covered account: (1) an account offered or maintained by MIT primarily for personal, family, and household purposes that involves or is designed to permit multiple payments or transactions; and (2) any other account offered or maintained by MIT for which identity theft is a reasonably foreseeable risk that may impact MIT's customers or the safety and soundness of MIT, including financial, operational, compliance, reputation, or litigation risks. An MIT example of a "covered account" is a student loan.

If the covered account is provisioned by or processed by a third party, then the guidance regarding third parties may apply (see section VII C). Where is it unclear whether an activity constitutes a covered account, business process owners should consult with MIT's Office of the General Counsel.

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 therefore.

Creditor: any person or business who arranges for the extension, renewal, or continuation of credit with a covered account. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. An MIT example of a "creditor" is Student Financial Services.

Customer: any person with a covered account with a creditor. An MIT example of a "customer" is a student who obtains a student loan.

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

Identifying Information: any information that is requested in conjunction with a covered account that may be used alone, or in conjunction with any other information, to identity a specific person.

Program Administrator: the Committee designated by MIT senior management to have primary responsibility for the implementation and oversight of the Program. See Section VII below.

Red Flag: a pattern, practice, or specific activity that indicates the possible existence of identity theft. The FTC regulations provide a list of 26 common red flags; organizations may decide that some of these 26 are not applicable, and/or that other red flags are more useful.

It should also be noted that the provisions MIT has for compliance with the Gramm-Leach-Bliley Act also apply in as much as MIT gathers personal, family, or household financial information that is not public, when that information relates to certain financial products or services they receive from MIT. Examples of such financial products or services include the TechCash feature of the MIT Card; the extension of credit for personal, family, or household loans and the servicing and collection of such loans, including student loans, faculty housing loans, and education loans for faculty and staff; financial or tax advice to prospective donors; and real estate or personal property leased for personal, family, or household use (but not including dormitory rooms or parking spaces).

IV. IDENTIFICATION OF RED FLAGS

In order to identify relevant red flags, MIT considers:

1. the types of accounts that it offers and maintains;
2. the methods it provides to open its accounts;
3. the methods it provides to access its accounts;
4. the usage of credit reports; and
5. previous experiences with identity theft.

MIT 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 individual;
3. Notice or report from a credit agency of an active duty alert for an individual; and
4. Indication from a credit report of activity that is inconsistent with an individual'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 description is not consistent with the person presenting the document;

3. Other documents with information that is not consistent with existing personal information (such as if a person's signature does not match between different documents, or does not match signature on file); and

4. Application 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 individual 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);

5. Social security number presented that is the same as one given by another individual;

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;

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

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

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. Mail sent to the account holder is repeatedly returned as undeliverable;

4. Notice to MIT that the individual is not receiving mail sent by MIT;

5. Notice to MIT that an account has unauthorized activity;

6. Breach in MIT's computer system security; unauthorized access to or use of individual account information.

E. Alerts from Others

Red Flag

1. Notice to MIT from an individual, 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.

V. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the red flags identified above associated with the opening of a **new covered account**, MIT personnel will take steps to obtain and verify the identity of the person opening the account. Each business unit responsible for offering covered accounts is expected to document the steps they will take, considering methods such as:

1. Requiring certain identifying information such as name, date of birth, address, driver's license, MIT ID, or other identification, and, where feasible, to compare with existing file information for the individual;

2. Verifying the identity (for instance, examine the picture on the MIT ID card); and

3. Independently contacting the purported individual, using contact information already on file in MIT systems (e.g., SAP).

B. Existing Accounts

In order to detect any of the red flags identified above for an **existing covered account**, MIT personnel will take steps to monitor transactions with an account. Each business unit responsible for monitoring covered accounts is expected to document the steps they will take, considering methods such as:

1. If an individual is requesting information in person, or via telephone, fax, or email, then verifying the identification of the individual prior to providing the information;

2. Verifying the validity of requests to change billing addresses, and/or confirming changes, such as sending change confirmation to email address on file; and

3. Verifying changes in banking information given for billing and payment purposes, such as contacting the individual via information already on file, prior to making any changes.

VI. RESPONDING TO RED FLAGS TO MITIGATE IDENTITY THEFT

In the event MIT personnel detect any identified red flags, such personnel shall take one or more of the following steps, after consulting with department management and depending on the degree of identity theft risk posed by the red flag:

A. Prevent and Mitigate

1. Contact the affected individual, using information already on file;

2. Change any passwords or other security devices that permit access to accounts;

3. Continue to monitor an account for evidence of identity theft;

4. Not open a new account;

5. Close an existing account;

6. Reopen an account with a new number;

7. Notify infoprotect@mit.edu to have the incident logged, and for additional assistance if needed;

8. Determine that no response is warranted under the particular circumstances.

B. Protect Personally Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to MIT accounts, MIT staff will adhere to MIT's policies and practices regarding protection of personal information.

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing, and updating this Program lies with the Program Committee, under the sponsorship and oversight of the Executive Vice President & Treasurer, and comprised of representatives of the Office of General Counsel, Audit Department, and Information Services & Technology, working in consultation with key business process owners, such as Student Financial Services.

The Committee will be responsible for the Program administration, for ensuring appropriate training of MIT staff on the Program, 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 circumstances, and considering periodic changes to the Program. The Committee will annually report to MIT's Audit Committee.

B. Program Updates

This Program will be periodically reviewed and updated to reflect changes in risks to individuals and the soundness of MIT's plan to protect individuals from identity theft. At least annually, the Program Committee will consider MIT's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts MIT maintains, and changes in MIT's business arrangements with other entities. After considering these factors, the Program Committee will determine whether changes to the Program, including the listing of red flags, are warranted. If warranted, the Program Committee will recommend updates to the Program, pending Executive Vice President & Treasurer approval.

C. Staff Training and Reports

MIT staff responsible for 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. Areas with covered accounts will review the Program at least annually, incorporating any Program updates in their local processes. New employees are expected to be trained prior to any involvement with covered accounts. Staff are expected to report any suspicious activity to infoprotect@mit.edu; this will automatically create a record in the reporting system. The Program Committee will prepare an annual review of the Program, including compliance and effectiveness.

D. Service Provider Arrangements

In the event MIT engages a service provider to perform an activity in connection with one or more covered accounts, MIT will take 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. This may include a review of the service provider's Red Flag Identity Theft Program, or contract language with regard to policies and procedures. Additionally, MIT and the service provider should have a mutually agreeable means for notification in the event the service provider identities a red flag situation.