Middlebury College Identity Theft Prevention Program

I. PROGRAM ADOPTION

Middlebury College has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. *See* 16 C. F. R. § 681.2. The College's Associate Vice President for Student Financial Services (referred to in this Program as the "Program Administrator") is responsible for the continued development of this Program, in consultation with appropriate College administrators and staff members. After consideration of the size and complexity of Middlebury College's operations and account systems, and the nature and scope of Middlebury College's activities, it was determined that this Program was appropriate for Middlebury College. This Program has been approved initially by the Risk Committee of the Board. The Risk Committee has delegated further responsibility for periodic review of this Program to the Controller of the College.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

This Program has been tailored to the size, complexity and the nature of the College's operations. The Program contains reasonable policies and procedures designed 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 the College from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person without authority" and a "Red Flag" as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

The Rule defines a creditor is "any person or business who arranges for the extension, renewal, or continuation of credit" with a "covered account." "Covered accounts" at Middlebury College (including Middlebury Institute of International Studies at Monterey) include, but are not limited to: The Federal Perkins Loan Program; The College Loan Program (including Fletcher Loan); Payment Plans toward the comprehensive fee(FACTS-Nelnet); Faculty Housing Loans; and the Chaplain's Fund. 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 it is

unclear whether an activity constitutes a covered account, the department should consult with the Program Administrator or designee(s)..

"Identifying information" is defined under the Rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including but not limited to: 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.

A "consumer report" as discussed below includes a criminal background check, credit check or other background check performed at the College's request by a third-party consumer reporting agency regarding a job applicant or prospective volunteer.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, Middlebury College 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, the usage of credit reports, and its previous experiences with Identity Theft. Middlebury College 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;
4. Receipt of a notice of address discrepancy from a consumer reporting agency from which the College has obtained a "consumer report" (e.g., a criminal background check or credit check done with a job applicant's or prospective volunteer's consent); and
5. 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 document with information that is not consistent with existing personal information (such as if a person's signature on a check appears forged, or a parent's signature does not match between different documents); and
4. Application for loan 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 or phone number 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 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 (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 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 Middlebury College that the individual is not receiving mail sent by Middlebury College;
5. Notice to Middlebury College that an account has unauthorized activity;
6. Breach in Middlebury College's computer system security; and
7. Unauthorized access to or use of individual account information.

E. Alerts from Others

Red Flag

1. Notice to Middlebury College 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.

IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account (e.g., enrollment of a new student), Middlebury College 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, address, driver's license, Middlebury College ID, or other identification;
2. Verify the identity (for instance, examine the Middlebury ID card);
3. Independently contact the purported individual, using contact information already on file in Middlebury College systems.

B. Existing Accounts

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

Detect

1. Verify the identification of individuals who request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer Report Requests

In order to deal with notices of address discrepancies received by the College from consumer reporting agencies from which the College has obtained "consumer reports" (e.g., a criminal background check or credit check done with a job applicant's or prospective volunteer's consent), the College has adopted the following policy and procedures.

1. The College will require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the consumer report is made to the consumer reporting agency; and

2. In the event that notice of an address discrepancy is received by the College from the consumer reporting agency, the College will verify that the consumer report pertains to the applicant or prospective volunteer for whom the report was made (by, for example, comparing the information in the consumer report with information that the College maintains in its own records or obtains from third-party sources, and/or consulting with the applicant or prospective volunteer), and report to the consumer reporting agency an address

for the applicant or prospective volunteer that the College has reasonably confirmed is accurate.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Middlebury College 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 risk posed by the Red Flag:

Prevent and Mitigate

1. Contact the Program Administrator or designee(s) for advice as to how to proceed;
2. Contact the individual;
3. Change any passwords or other security devices that permit access to accounts;
4. Continue to monitor an account for evidence of Identity Theft;
5. Not open a new account;
6. Close an existing account;
7. Reopen an account with a new number;
8. Contact law enforcement; and/or
9. Determine that no response is warranted under the particular circumstances.

Protect personally identifying information

Middlebury College maintains a comprehensive written information security plan-please see http://www.middlebury.edu/offices/technology/security/infosecphilosophy.

VI. PROGRAM ADMINISTRATION

.

A. Oversight of the Program

The Program Administrator was responsible for developing, and will be responsible for implementing and updating, this Program. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Middlebury College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, for determining (personally or through designees) which steps of prevention and mitigation should be taken in particular circumstances, and for considering periodic changes to the Program. The Program Administrator may appoint two or more College administrators or staff members to an Identity Theft Prevention Committee ("Committee") chaired by the Program Administrator, which Committee may assist the Program

Administrator in carrying out such duties. The Program Administrator will, nonetheless, retain ultimate responsibility for such duties.

B. Updating the Program

This Program will be periodically reviewed and updated to reflect changes in risks to individuals and the soundness of Middlebury College's plan to protect individuals from Identity Theft. At least annually, the Program Administrator will consider Middlebury College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts that Middlebury College maintains, and changes in Middlebury College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. In carrying out these duties, the Program Administrator may consult with and/or gather information from the Committee, College administrators, staff, vendors and other individuals or firms as appropriate and necessary.

C. Staff Training

Middlebury College staff members responsible for implementing the Program shall be trained by the Program Administrator, Committee members and/or designees in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Training will be done as necessary to effectively implement the program.

D. Service Provider Arrangements

In the event that Middlebury College engages a service provider to perform an activity in connection with one or more covered accounts, Middlebury College 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 Middlebury College's Program and report any Red Flags to Middlebury College's Program Administrator or designee(s), and/or take appropriate steps to prevent or mitigate identity theft.