Hampshire College Identity Theft Program

Issued: March 29, 2011

Responsible Official: Vice President for Finance and Administration, Treasurer

1.0 Purpose

Hampshire College (the College) recognizes that some of its activities are subject to the provisions of the Federal Fair and Accurate Credit Transactions (FACTA) and the Federal Trade Commission's so-called Red Flag rules. The purpose of this program is to provide information to assist individuals in the detection, prevention, and mitigation of Identity Theft in connection with the opening of a Covered Account (as that term is defined below) or any existing Covered Account. This program also provides guidance to employees who believe that a breach of security incident may have occurred and with the protocol and process for reporting of such a security incident.

Under the Red Flag rules, the College is required to establish an "Identity Theft Program" with policies and procedures appropriate to the College's size and complexity in order to detect, identify, and mitigate identity theft in its Covered Accounts. These "Red Flags" are noticed inconsistencies in specific financial transactions which should indicate the need for further investigation. The College must incorporate relevant Red Flags rules into a Program to enable the College to detect and respond to potential Identity Theft.

2.0 Definitions

An **Account** is a continuing relationship established by any person(s) and the College to obtain a product or service from the College for personal, family, household or business purposes.

A **Covered Account** is any Account offered and/or maintained by the College acting as a creditor (1) that involves or is designed to permit multiple payments or transactions for personal, family, or household purposes; or (2) for which there is a reasonable foreseeable risk of harm to the person holding an account or to the College from identity theft - for example, small business or sole proprietorship accounts.

The College acts as a **creditor** when it regularly extends, renews or continues credit regarding an Account. Examples include, but are not limited to, tuition, room and board, lab fees, meal plans, bookstore charges, computer loans, etc.

The College has identified the following Covered Accounts:

<u>College administered Covered Accounts – Students:</u>

- Plus Loans (the College is a direct lender; collection is performed by the U.S. Government);
- Stafford Loans (the College is a direct lender; collection is performed by the U.S. Government); and
- Student Accounts.

College administered Covered Accounts – Employees:

- Computer loans;
- Employee receivables (meal charges and bookstore charges); and
- Outstanding employee mortgages.[1]

Service provider Covered Accounts:

- Tuition Management Services (TMS) Monthly Payment Plan;
- Affiliated Computer Services (ACS) – Perkins Loans;
- Employee flexible spending plans – Benefit Strategies; and
- Collection Agencies.

Identity theft is an attempted or committed act of fraud using the identifying information of another person without that person's authority for the purpose of effecting a transaction involving a Covered Account.

Identifying information is any name or identity related number that may be used alone or in conjunction with other information to identify a specific person. Examples include, but are not limited to, social security numbers, driver license numbers, credit card numbers, dates of birth, addresses, phone numbers, maiden names, names, account number(s), student numbers, employee numbers, credit card expiration dates, cardholder names, cardholder addresses, taxpayer identification numbers, employer identification numbers.

A **Red Flag** is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

A **service provider** is any third party that provides services to the College in support of its offering, opening and administration of Covered Accounts.

3.0 Identifying Red Flags

The following Red Flags are potential indicators of fraud. Red Flags are not limited to these examples. Any time a Red Flag, or a situation closely resembling a Red Flag is apparent, it must be investigated by appropriate person(s). Red Flags include, but are not limited to:

- Documents provided for identification appear to have been altered or forged;
- Presentation of student or employee information that is inconsistent with information in the College's information systems or regularly kept business records;
- Inaccurate personal identification information, or personal identification information that is inconsistent with the College's business records, such as social security numbers or addresses;
- Alerts, notifications or other warnings received from service providers, such as fraud detection services, student loan administrators, banks or other third-party entities who have access to College-maintained information;
- Suspicious documents (i.e., the photograph or physical description of the identification is not consistent with the appearance of the individual presenting the identification)

[1] The College no longer provides new employee mortgages.

- Unusual or suspicious activity in any Covered Accounts;
- Notices from customers, victims of identity theft, the Public Safety Department or other law enforcement authorities regarding possible identity theft;
- Requests to mail information to an address not listed in the College's business files;

4.0 Procedures for Detecting Red Flags

The College's procedures for detecting Red Flags are as follows:

- **Identification cards.** Staff members are responsible for recognizing the proper appearance of College-issued identification cards. If there appear to be any problems with any card presented to transact in connection with a Covered Account (i.e., if the card appears to be forged, altered or subject to any other Red Flags above), or if a card is reported missing or stolen, staff members shall seek a second form of identification (i.e., driver's license); to verify personal information consistent with the information in the College's files before providing any access to sensitive information, allowing the person to transact in connection with a Covered Account, or giving a student/employee a refund check.)
- **Student and employee loan accounts and accounts receivable.** Account disbursements and credits are handled automatically through the College's computer systems, which are protected through information technology monitoring systems and security. Student Financial Services and Human Resources/Payroll have in place and shall maintain a verification system requiring individuals seeking information to provide appropriate authentication information (i.e., a valid identification) consistent with this Policy.
- **Third party vendors.** The College shall take reasonable steps consistent with this Policy to verify that its third party vendors have the capacity to protect personal information in accordance with Massachusetts law. If a third party vendor is shown not to be able to protect personal information in a manner consistent with the requirements of this Policy, the College will take all appropriate legal action.
- **Receipts of Red Flag notices from third party entities.** All staff members who may receive notices of security breaks or Red Flag notices from law enforcement agencies, service providers, students or employees, are and shall be instructed to direct the notice to his or her department manager, who will then promptly report the receipt of the notice to the Controller.

5.0 Response to Red Flags

When a Red Flag is detected or reported, the following procedures must take place as soon as practicable:

1. The Controller will notify the Vice President for Finance and Administration and the Five College Risk Manager.
2. The Controller will perform an initial risk assessment.
3. Upon completion of the risk assessment, the holder of the Covered Account will be notified and the appropriate department (Financial Services/Human Resources/Payroll) will implement any needed changes to existing security measures, including but not limited to changing passwords, security codes or other security devices that permits access to the Covered Account and/or closure of the Account.
4. The appropriate College administrators, including without limitation, the Controller, Five College Risk Manager, and/or Director of Information Technology, will determine whether

any additional steps are necessary. Additional action steps may include: notification of law enforcement administration or officials of the suspected fraud; notification to appropriate outside service providers; notification to Covered Account holders; or notice to the Board of Trustees Audit Committee.

6.0 Oversight

1. **Overall Program.** The Vice President for Finance and Administration is responsible for the development, implementation, oversight and continued administration of the Identity Theft Detection Program.
2. **Service Providers.** The College requires all of its service providers that may have access to identifying information (see definition above) to implement their own Red Flags policies and to provide the College with timely written notice of Red Flags relating to College information. If a third party vendor fails either develop and maintain or operate in a manner consistent with its policies regarding identity theft, the College will take all appropriate legal action.
3. **Annual Reporting/Updates.** The Controller will review the College's compliance with this program annually, including an updated assessment of institutional risk, and recommend any necessary modifications to the program to the Vice President for Finance and Administration.

7.0 Staff Training

College staff who have responsibilities in the establishment of student or employee Accounts or identification cards, as well as those staff involved with the Covered Account, must successfully complete Identity Theft Training.