HAMILTON COLLEGE

Identity Theft Prevention Program
Policy Statement

Effective Date: June 6, 2009

Background

This policy establishes a program to detect, prevent and respond to "Red Flags" which could signal potential identity theft in connection with the opening and/or maintenance of accounts maintained by Hamilton College. It supplements the College's existing policies that protect student information and records, employee information, financial accounts, information technology services, and related sensitive information maintained by the College. This policy was established to comply with the provisions of the Federal Trade Commission's ("FTC") regulations on Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

All Hamilton College employees have a fiduciary responsibility to refrain from discussing confidential matters regarding our "customers", defined as any third party engaged in a financial transaction with the College. Employees who have access to personal information such as social security numbers or credit card information must insure that the information is safeguarded in a locked space.

Definitions

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

Identity Theft: An attempt to commit or a committed fraud using the identifying information of another person without that person's authority.

Identifying Information: Any name or number that may be used alone or in conjunction with other information to identify a specific person. Examples include names, social security numbers and driver's licenses.

Account: A continuing relationship established by any person with the College to obtain a product or service from the College for personal, family, household, or business purposes.

Service Provider: Any third party that provides services to the College. Service providers of the College relating to this program include providers of student and employee health insurance, third-party retirement and other benefits administrators, financial institutions that administer the College's tuition payment plan programs, governmental and private student loan providers, electronic billing and payment partners, and collections agencies.

Covered Account: An account offered or maintained by the College, acting as a creditor, that is used primarily for personal, family, or household purposes and involves or is designed to permit multiple payments or transactions, *or* an account for which there is a reasonably foreseeable risk of harm to the account holder or the College from identity theft.

Covered Account Holder: Any person who has a covered account with the College

Credit: The right granted to a person by the College to defer payment of debt or to purchase goods or services and defer payment.

Identity Theft Prevention Program

I. Identification of Red Flags

The Red Flag regulations require the College to perform an assessment of the potential risk of identity theft associated with its Covered Accounts. The assessment must be based in part on the College's history with identity theft incidents. The College has not had any previous reported serious incidents of identity theft on any of these Covered Accounts**.** Hamilton therefore assesses the probability of identity theft problems as low. Nevertheless, every employee must be vigilant to potential Red Flag violations.

The College considers the following factors in identifying Red Flags for Covered Accounts:

1. The types of Covered Accounts which the College offers and/or maintains
2. The methods the College uses to open accounts
3. The methods the College allows to access its Covered Accounts
4. Any previous problems with identity theft involving College accounts
5. The methods the College allows to update or change information with respect to its Covered Accounts.

The College has determined that the following accounts may constitute Covered Accounts:

1. The College's campus card ("Hill Card") which permits cardholders to access a variety of College services
2. Deferment of tuition payments, including TuitionPay, a payment plan administered by Sallie Mae
3. Student loan accounts including Perkins and Institutional loans and accounts administered by ACS, Inc., a servicer of student loans
4. Employee loan accounts including mortgage loans, the Love loan and computer loans
5. Charitable contributions paid in installments.

Employees should look for the following types of Red Flags:

1. Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
2. The presentation of suspicious, forged or altered documents or identifying information
3. Unusual or suspicious activity in a covered account
4. Notice of possible identity theft from the Covered Account holder, law enforcement authorities or third parties

II. Detection of Red Flags

For the College's purposes, Red Flags may include, but are not limited to: documents that appear forged; presentation of student or employee information which is inconsistent with information in storage; inaccurate personal identification information, 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; suspicious personal identifying information; unusual activity in Covered Accounts; or notices from campus safety, students, employees, or law enforcement authorities regarding identity theft.

The College's procedures for detecting Red Flags with respect to Covered Accounts are as follows:

a. The campus card ("Hill Card") - Hamilton employees have the responsibility of recognizing the appearance of College-issued cards. A second form of identification is required if there are any problems with the cards, or if a card is reported as missing or stolen. If a student or staff member seeks access to sensitive information but cannot produce identification, the student or staff member will be asked to provide other means of self-identification, such as validating other personal information available in the College systems.
b. Student accounts and TuitionPay - Requests must be made in person or in writing and personal identifying information must be provided.
c. Student and employee loan accounts - Requests must be made in person or in writing and personal identifying information must be provided. Disbursements are mailed to the address on file or picked up in person by presenting a photo ID.
d. Receipts of Red Flag notices from third party entities, such as banks. The College has instructed all employees who may receive such notices that security breach or Red Flag notices from law enforcement, service providers, students, or employees will be directed to the employee's immediate supervisor, who will then report the receipt of the notice to the Business Office

III. Responding to Red Flags

When a Red Flag is detected by or reported to a College employee:

1. An initial risk assessment of the particular Red Flag will be performed by the Controller.

2. The holder of the covered account will be notified and the Business Office will implement any necessary enhanced security measures, including but not limited to, account closure.
3. The Controller, in consultation with the Vice President, Administration and Finance, will determine whether notification of law enforcement officials or involvement of Campus Safety is necessary.
4. The Business Office will respond appropriately to prevent future identity theft breaches, including but not limited to notification of information technology professionals within the College or at service providers who can change passwords or otherwise increase electronic security.

IV. Oversight

Service Providers: The College requires all of its service providers which may have access to the College's sensitive information to implement their own Red Flags policies and to provide the College with timely written notice of the detection of Red Flags that could potentially affect the College's Covered Accounts. The College collects and maintains on file, documents from Service Providers that confirm compliance with the Red Flag rules.

V. Annual Reporting and Maintenance

The Controller and the Vice President for Administration and Finance will annually review the College's compliance with this policy to determine whether all aspects of the program are up to date and applicable. They will implement any necessary updates to the policy and report to the College's Board of Trustees as needed.

The Controller or his/her designee is authorized to supplement the Covered Accounts assessment in this policy periodically as needed and to inform any new or additional service providers of this policy.

Address Discrepancy Notifications and Changes of Address

The regulations pursuant to FACTA also require the College to establish a process for handling address discrepancy notifications received in connection with its use of consumer credit reports. Departments that use consumer credit reports for employment purposes shall develop policies and procedures for responding to notices of address discrepancy received from the consumer reporting agency. These procedures shall ensure that the department is able to form a reasonable belief that the requested consumer report relates to the actual individual for which it is intended. Departmental procedures may include verifying information in the consumer report with the individual and / or with College records and verifying information with documents provided by the employee or third parties.