**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

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