

# Carleton College

## IDENTITY THEFT PREVENTION PROGRAM POLICY STATEMENT

### Program Adoption

Carleton College developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission’s (FTC) Red Flags Rule, set forth in Part 681 of Title 16 of the Code of Federal Regulations which implements Section 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. After consideration of the size of the College’s operations and account systems, and the nature and scope of the College’s activities, senior management determined that this Program was appropriate for Carleton College, and approved this Program in February 2009.

### Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Policy. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts offered or maintained 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.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

### Definitions

**Identity Theft** means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** is:

1. An account offered or maintained by the College, *acting as a creditor*, primarily for personal, family or a household purpose that involves or is designed to permit multiple payments or transactions.
2. A **Red Flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

### Covered Accounts

Located on the I-Drive (Collab)/Departments/Busi/Business Office/Business Office Documents/Policies/2008-2009 Identity Theft Prevention Policy

# Carleton College

## IDENTITY THEFT PREVENTION PROGRAM POLICY STATEMENT

Carleton College has identified six types of accounts, four of which are covered accounts administered by the College and two types of accounts that are administered by service providers.

College covered accounts:

1. Refund of credit balances involving PLUS loans
2. Refund of credit balances, without PLUS loans
3. Student accounts
4. Emergency loans

Service provider covered accounts:

1. TuitionPay, a payment plan administered by Sallie Mae, and
2. ACS, Inc. administers the Perkins loans, Henry Strong Loan and Carleton College Loan repayments

Please refer to “**Oversight of Service Provider Arrangements**” on page 4.

### **Identification of Relevant Red Flags**

The program considers the following risk factors in identifying relevant Red Flags for covered accounts:

1. The types of covered accounts as noted above;
2. The methods provided to open covered accounts—acceptance to the College and enrollment in classes requires all of the following information:
  - a) Common application with personally identifying information
  - b) High school transcripts or prior college transcripts
  - c) Official ACT, SAT, AP and/or IB scores
  - d) Two letters of recommendation
  - e) Entrance Medical Record
  - f) Medical history
  - g) Immunization history
  - h) Proof of Insurance
3. The methods provided to access covered accounts:
  - a) Disbursements obtained in person require photo identification
  - b) Disbursements obtained by mail can only be mailed to an address on file
4. The College’s previous history of identity theft.

The program identifies the following Red Flags:

1. Documents provided for identification appear to have been altered or forged;

Located on the I-Drive (Collab)/Departments/Busi/Business Office/Business Office Documents/Policies/2008-2009 Identity Theft Prevention Policy

# Carleton College

## IDENTITY THEFT PREVENTION PROGRAM POLICY STATEMENT

2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request made from a non-College issued E-mail account;
4. A request to mail something to an address not listed on file; and
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

### Detection of Red Flags

1. **Refund of a credit balance involving a PLUS loan** – As directed by federal regulation (U.S. Department of Education) these balances are required to be refunded in the parent's name and mailed to their address on file within the time period specified. No request is required. **Red Flag** - none of this is initiated by the College.
2. **Refund of credit balance, no PLUS loan** – requests from current students must be made in person by presenting a photo ID or in writing from the student's college issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing photo ID. Requests from students not currently enrolled or graduated from the college must be made in writing. **Red Flag** – Photo ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
3. **Student accounts** – requests must be made in person by presenting a photo ID or in writing from a college issued e-mail account. **Red Flag** – Photo ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
4. **Emergency Loan** – Requests must be made in person by presenting a photo ID or in writing from the student's college issued e-mail account. The loan check can only be mailed to an address on file or picked up in person by showing photo ID. **Red Flag** – Photo ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
5. **Tuition payment plan** – Students must contact an outside service provider and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.
6. **Loan Service Provider** - Students must contact an outside service provider and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.

### Response

The Program shall provide for appropriate responses to detected Red Flags to prevent and mitigate identity theft. The appropriate responses to the relevant Red Flags are as follows:

Located on the I-Drive (Collab)/Departments/Busi/Business Office/Business Office Documents/Policies/2008-2009 Identity Theft Prevention Policy

# Carleton College

## IDENTITY THEFT PREVENTION PROGRAM POLICY STATEMENT

1. Deny access to the covered account until other information is available to eliminate the Red Flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

### **Oversight of the Program**

Responsibility for developing, implementing and updating this Program lies with the College Comptroller. The Comptroller will be responsible for the Program administration, for ensuring appropriate training of College's 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.

### **Updating the Program**

This Program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the College from identity theft. At least once per year in September, the Comptroller will consider the College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the College's business arrangements with other entities. After considering these factors, the Comptroller will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Comptroller will update the Program.

### **Staff Training**

College staff responsible for implementing the Program shall be trained either by or under the direction of the Comptroller in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

Training has been embedded into the online FERPA web tutorial incorporated into new staff orientation and training provided by the Human Resources Office.

### **Oversight of Service Provider Arrangements**

The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity

# **Carleton College**

## **IDENTITY THEFT PREVENTION PROGRAM POLICY STATEMENT**

theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Currently the College uses Sallie Mae to administer the Tuition Payment Plan and ACS to administer the Perkins; Henry Strong and College Loans. Students contact Sallie Mae or ACS directly via the internet or by telephone and provide personally identifying information to be matched to the records that the College has provided to Sallie Mae and ACS.

Personally identifying information transmitted to or from Sallie Mae and ACS is done through a secure web portal and/or data encryption technology.