Community College System of New Hampshire Identity Theft Prevention Program

Revised 5/4/2009

Program Adoption

The Community College System of New Hampshire ("CCSNH") 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. This program was developed with oversight and approval of various CCSNH committees with approval of the program by the CCSNH Chancellor and System Leadership Team in May 2009. You can read the full CCSNH Red Flags Policy here.

Purpose of the Program

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 Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts the colleges offer or maintain 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 students and to protect the safety and soundness of the creditor from identity theft

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

Definitions

- **Identify theft**: Fraud committed or attempted using the identifying information of another person without their authority.
- **Red flag**: A pattern, practice or specific activity that indicates the possible existence of identity theft.
- **Covered account**: An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Examples identified by CCSNH include, but are not limited to:

  - College covered accounts:
    - Refund of credit balances involving PLUS loans

    - Refund of credit balances, without PLUS loans
    - Deferment of tuition payments
    - Emergency loans

- System Office covered accounts:
    - CCSNH Foundation
    - Technical Education Loan

- Service provider covered accounts:
    - Tuition payment plans administered by ECSI, Nelnet, FACTS or other providers (refer to "Oversight of Service Provider Arrangements")

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 require the following information:
    a. Registration Form and/or Application for Admission with personal identifying information
    b. Any other documents required by the College for course registration or admission to the college and/or academic program
3. The methods provided to access covered accounts:
    a. Disbursements obtained in person require picture identification
    b. Mailed disbursements may only be mailed to an address on file with the college
4. The College's previous history of identity theft.

Red Flags Identified by the Program:

1. Documents provided for identification which appear to have been altered or forged
2. The photograph or physical description on the identification is not consistent with the appearance of the student, faculty or staff person 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
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

The Program will detect red flags relevant to each type of covered account as follows:

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. Red Flags:
    a. None as this is initiated by the Colleges and federally mandated to be mailed to the parent's address.
2. Refund of credit balance, non PLUS loan –The refund check can only be mailed to an address on file with the college. Red Flags:
    a. Students who change addresses frequently
    b. Colleges that accept change of addresses over the telephone or without proper ID
    c. Colleges that accept address changes from a non college email address
3. Deferment of tuition payment – request is made in person only and requires the student's signature. Red Flag:
    a. none.
4. Emergency loan - Requests must be made in person by presenting a picture 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 picture ID. Red Flag:
    a. Picture ID not appearing to be authentic or not matching the appearance of the person presenting it
    b. Request coming from a non CCSNH e-mail account
5. Tuition payment plan – Students must contact an outside service provider and provide personally identifying information to them. Red Flag:
    a. none, see Oversight of Service Provider Arrangements below

Program Response

This 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:

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

Oversight of the Program

Responsibility for developing, implementing and updating this Program lies primarily with the Finance Office in the Systems Office (Program Administrators). The Chief Financial Officers, or CFOs, will be Program Coordinators for each campus. The Program Coordinators will work in collaboration with their campus staff and the CCSNH Finance Office to ensure the appropriate training of College's staff on the Program, for reviewing and appropriately responding to any staff reports regarding the detection of Red Flags, identifying steps for preventing and mitigating identity theft in particular circumstances and recommending periodic changes to the Program.

Updating the Program

This Program will be periodically reviewed and updated by the appropriate CCSNH committees to reflect changes in risks to students and the soundness of the College from identity theft. At least once per year, normally in October, the Program Administrators in collaboration with the campus CFOs 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 Program Administrators will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrators will update the Program.

Staff Training

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

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

Current Contracts with Service Providers (2009):

1. CCSNH employs Educational Computing Services Inc. (ECSI), a Perkins Loan servicer for the purpose of billing and collection of Perkins and college loan payments. The only information that is shared with ECSI is information required to properly bill and collect loan payment as established by the Department of Education. This includes student name, address, telephone number, social security number, and date of birth. CCSNH will keep a copy on file of ECSI's compliance with FTC Red Flag Rules. CCSNH has also enrolled in ECSI's Red

Flag Regulation Services which provides tagging and reporting of suspicious activity (multiple address changes, attempts to get information by calling in) on our accounts.

2. Online Payment Provider. CCSNH’s Online Payment Provider is required to be PCI compliant. PCI Compliance consists of a set of "Industry Security Requirements" adopted by the Payment Card Industry to ensure credit card transactions are secure.