Quinsigamond Community College
A community of support. A world of possibilities.

REQUEST FOR BOARD OF TRUSTEES ACTION

Committee: Audit and Oversight

Title: Adoption of Identity Theft Prevention Guidelines

Date: May 13, 2009

Recommendation: That the Board of Trustees approved the proposed Identity Theft Prevention Guidelines.

Justification: Following the recommendation issued by the Office of the Community College Council, the attached Identity Theft Prevention Guidelines were prepared from a template produced through the collaboration among the Comptrollers of the fifteen community colleges for adoption individually by each campus throughout the system.

Quinsigamond Community College
Identity Theft Prevention Program

PROGRAM ADOPTION

Quinsigamond Community College ("College") 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 the Audit and Oversight Committee of the Board of Trustees. After consideration of the size of the College's operations and account systems, the nature and scope of the College's activities, the Board of Trustees determined that this Program was appropriate for the College, and therefore approved this Program on May 13, 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 Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains 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 the safety and soundness of the creditor from identity theft.

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

DEFINITIONS

Red Flags Rule Definitions Used in this Program:

"Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."

A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

A "Covered Account" is an account that the College maintains, primarily for personal, family or household purposes that involves, or is designated to permit multiple payments or transactions.

The "Program Administrator" is the individual designated with primary responsibility for oversight of the program.

"Identifying Information" is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

COVERED ACCOUNTS

Springfield Technical Community College has identified four types of accounts, three of which are covered accounts administered by the College and one type of account that is administered by a service provider.

College covered accounts:

1. Refund of credit balances involving PLUS loans
2. Refund of credit balances, without PLUS loans
3. Deferment of tuition payments

Service provider covered account:

1. Tuition payment plan administered by a third party, refer to "Oversight of Service Provider Arrangements on page 5.

IDENTIFICATION OF RELEVENT 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 transcript
   c) Official ACT or SAT scores
   d) Entrance Medical Record
   e) Medical history
   f) Immunization history
   g) Insurance card
3. The methods provided to access covered accounts:
   a) Disbursement obtained in person require picture 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. Documentation provided for identification appears to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. Other documents with information that is not consistent with existing student information;
4. A request made from a non-College issued E-mail account;
5. A request to mail something to an address not listed on file;
6. Notice from customers, victims of identity theft, law enforcement authorities, consumer reporting agencies, or other persons regarding possible identity theft in connection with covered accounts;
7. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
8. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
9. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent; and
10. Social security number presented that is the same as one given by another student.

DETECTION OF RED FLAGS

The Program will detect red flags relevant to each type of covered accounts 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. No request is required. **Red Flag** – none as this is initiated by the College.
2. **Refund of credit balance, no PLUS loan:** Requests from current students may be made in person by presenting a picture 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 picture ID. Requests from students not currently enrolled or graduated from the college must be made in writing. **Red Flag** – Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Requests not coming from a student issued e-mail account.
3. **Deferment of tuition payment:** requests are made in person, via e-mail, or via fax. **Red Flag** – Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Requests not coming from a student issued e-mail account. Identifying information presented is inconsistent with other sources of information.

4. **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.
5. **Any other covered account that may be identified by the Program Administrator:** Any alert notification or warning or notice of address discrepancy obtained through a combination of suspicious documents or personal identifying information identified as a red flag by College employees or brought to the attention of the College by a victim of identity theft, or by a consumer reporting agency.

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 may include:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Gather information to attempt to authenticate or determine if attempted transaction was fraudulent or authentic;
3. Contact the student;
4. Change any passwords, security codes or other security devices that permit access to a covered account;
5. Notify and cooperate with law enforcement;
6. Notify any credit reporting agency or third party, if applicable; or
7. Determine no response is warranted under the particular circumstances.

OVERSIGHT OF THE PROGRAM

Responsibility for the oversight of the Program will fall under the jurisdiction of the CFO/Vice President of Administrative Services. As designated by the CFO/Vice President for Administrative Services, a Program Administrator (Comptroller) will be responsible for the Program administration (developing, implementing, updating, monitoring) including ensuring appropriate training of the 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, the Program Administrator 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 Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program in consultation with the CFO/Vice President for Administrative Services.

STAFF TRAINING

College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator 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 polices 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.

Currently, the College uses Nelnet to administer the Tuition Payment Plan. Students contact Nelnet directly through its website or by telephone and provide personally identifying information to be matched to the records that the College has provided to Nelnet.