North Shore Community College

NORTH SHORE
COMMUNITY COLLEGE

"IDENTITY THEFT - RED FLAG RULE POLICY"

WHEREAS, The Federal Trade Commission has adopted Regulations 16 CFR 681 pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) known as the "Red Flags Rule"; and

WHEREAS, Those rules become effective May 1, 2009, and

WHEREAS, Those rules may be applicable to certain activities participated in by higher education institutions; and

WHEREAS, The Board of Trustees of North Shore Community College has determined that the following policy is in the best interest of the College and its employees, students, and contractors.

NOW, THEREFORE,

BE IT RESOLVED by the Board of Trustees of North Shore Community College (or appropriate subcommittee) that the following is hereby approved:

Program Adoption & Purpose

The North Shore Community College (NSCC) Red Flag Identity Theft Prevention Program (Program) has been developed and implemented in response to the regulation issued by the Federal Trade Commission (FTC) known as the Red Flag Requirements (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act). The program required by this regulation must detect, identify and respond to "patterns, practices, or specific activities-known as 'red flags' that could indicate possible "identity theft".

Definitions

<u>Identity theft</u>: Fraud committed or attempted using the identifying information of another person without authority.

<u>Covered Account</u>: A consumer account that involves multiple payments or transactions, such as a loan or account that is billed or payable monthly.

<u>Red Flag</u>: patterns, practices, and specific activities that signal possible existence of identity theft.

Program Administrator: The individual designated with primary responsibility for oversight of the program including annual review and training of the College's staff.

Identifying information: 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.

Scope of Covered Accounts

- NSCC Emergency Save Loans
- Installment Plans for covered student accounts
- Refund of credit balances involving PLUS loans
- Refund of credit balances, without PLUS loans
- Individual payment arrangements deemed necessary by Dean of Student Financial Services or the Coordinator of Student Accounts

Existing Policies and Practices

Many offices at North Shore Community College (NSCC) maintain files, both electronic and paper, of student biographical, academic, health, financial, and admission records. These records may also include student billing information and personal correspondence with students and parents. NSCC institutional policies ensure compliance with Family Educational Rights and Privacy Act (FERPA), and Payment Card Industry security standards (PCI). Risk of identity theft is also mitigated by internal control procedures and system & application security. Institutional Records are safeguarded to ensure the privacy and confidentially of student, parents, alumni and employees. The following are examples of how NSCC handles sensitive personal data:

- A FERPA disclosure statement is sent to students each semester informing them of their rights under FERPA. Students are required to give written authorization to the College in order to release non-directory information and/or confidential information, to a third party. Students are given the opportunity to provide billing addresses for third party billing (companies, scholarship foundations, etc).

- Occasionally, NSCC will extend short term credit to a student for payment of their tuition bill which thus creates a covered account. The student signs a short term promissory note, which is stored in a secured area. If we receive information of an address change (which is a red flag), we verify the change by contacting the student before making the change in the Banner system.

- Access to student data in NSCC's Banner system is provisioned to employees of the College based on business area and need to know to properly perform their job functions. These employees are trained to know FERPA and “Red Flag” regulations. . The inappropriate use of such access and/or use of administrative data may result in disciplinary action up to, and including, dismissal from the College.

- Social Security numbers are not used as identification numbers and this data is classified as non-directory information.

- Every effort is made to limit the access to private information to those employees on campus with a legitimate "need-to-know." NSCC Staff who have approved access to the administrative information databases understand that they are restricted in using the information obtained only in the conduct of their official duties

Identification of Relevant Red Flags for Covered Accounts

The Program recognizes relevant Red Flags for covered accounts from the following categories:

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 enforcements authorities, consumer reporting agencies, or other persons regarding possible identity theft in connection with covered accounts;

7. Identifying information that is inconsistent with other information the student provides (e.g., inconsistent birth dates);

8. Identifying information that is inconsistent with other sources of information (e.g., address given does not match address on 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 shall address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, as follows:

1. Confirming identifying information about, and verifying the identity of, a person opening a covered account.

2. Authenticating "customers", monitoring transactions, and verifying the validity of change of address requests.

Response

Should an employee identify patterns, practices and specific activities that signal possible identify theft ("Red Flag"), they are instructed to bring it to the attention of their immediate supervisor. The supervisor is responsible for reviewing the information and determining whether escalation is appropriate. If a decision is made that escalation is warranted, the VP of Administration and Finance will be notified immediately. Additional actions may include notifying and cooperating with appropriate law enforcement and notifying the student or employee of the attempted fraud.

The NSCC Program shall provide appropriate responses to detected red flags. These responses may include:

1. Monitor a covered account for evidence of identity theft.
2. Direct communication with the student.
3. Change any passwords, security codes or other security devices that permit access to a covered account.
4. Reopen a covered account with a new account number.
5. Not open a new covered account.
6. Close an existing covered account.
7. Notify law enforcement.
8. Determine no response is warranted.

Oversight of the Program

Responsibility for the oversight of the Program will fall under the jurisdiction of the Vice President of Administration and Finance. As designated by Vice President of Administration and Finance, a Program Administrator will be responsible for developing, implementing, updating and monitoring the Program. This includes:

- ensuring appropriate training of the College's staff,
- reviewing staff reports pertaining to the detection of red flags,
- determining the steps required for preventing and mitigating identity theft,

- considering periodic changes to the Program.

Updating the Program

The Program shall be updated periodically to reflect changes in risks to “customers” or to the safety and soundness of the organization from identity theft based on factors such as:

1. The experiences of the organization with identity theft.
2. Changes in methods of identity theft.
3. Changes in methods to detect prevent and mitigate identity theft.
4. Changes in the types of accounts that the organization offers or maintains.
5. Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Oversight of Service Provider Arrangements

NSCC is reviewing options for outsourcing the College Installment Plan. The Program will be updated to reflect any changes in this area.