Policy & Procedure No. FIN-020

Northshore Technical Community College

Title:	Identity Theft Prevention Program
Effective Date:	9/07/2017
Last Revision Date:	5/02/2017
Cancellation:	
Office:	Finance (FIN)

Identity Theft Prevention Program

PURPOSE

Northshore Technical Community College (NTCC) in response to the growing problem of identity theft and recognizes the need to safeguard personal and private information of all its constituents, including students, faculty, staff, vendors, and donors. The program has been designed to be appropriate to the size and complexity of the College and the nature and scope of its activities.

LCTCS BOARD POLICY & PROGRAM ADOPTION

LCTCS Policy #5.028 titled "Identity Theft Prevention Program" requires each of its colleges to establish an identity theft prevention program policy. LCTCS has determined that its institutions fall under the provisions of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Public Law 108-159; specifically sections 114 and 315. To ensure compliance with the Act, institutions under the auspices of the LCTCS shall develop and implement an appropriate policy an identity theft prevention program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account as defined in the Act. This program was developed with oversight and approval of the System Office. After consideration of the size of the System's operations and account systems, and the nature and scope of the System's activities, the Board of Supervisors determined that this Program was appropriate for the System.

DEFINITIONS

1. **Identity theft** is defined as fraud committed or attempted using the identifying information of another person without authority.
2. **Creditor** is any person or organization who regularly extends, renews, or continues credit; any person or organization who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.
3. **Covered Account** is 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.
4. **Red Flag** is a pattern, practice or specific activity that indicates the possible existence of identity theft.
5. **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 but not limited to: 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.

6. **Service Provider** means someone who provides a service directly to the financial institution or creditor.

COVERED ACCOUNTS

The following covered accounts are administered **by the System/College**:

1. Refund of credit balances
2. Loan Programs
3. Other accounts that may be identified by departmental units as meeting the definition of Covered Account

The following covered accounts are administered **by a service provider**:

1. Tuition payment plan administered by CashNet, refer to the Section labeled "Oversight of Service Provider Arrangements" within this policy.
2. Refund of credit balances by BankMobile, refer to the Section labeled "Oversight of Service Provider Arrangements" within this policy.

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;

***Alerts from Others**:*

1. Notice to the College from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.
2. Report of fraud accompanying a credit report;
3. Notice or report from a credit agency of a credit freeze on a customer or applicant;
4. Notice or report from a credit agency of an active duty alert for an applicant;
5. Notice or report from a credit agency of address discrepancy; and
6. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

Suspicious Documents:

1. Identification document or card that appears to be forged, altered, or not authentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (i.e. a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.
5. Other suspicious enrollment documentation including but not limited to:
   a. High school transcript
   b. Official ACT or SAT scores
   c. Letters of recommendation

d. Entrance medical record
e. Medical history
f. Immunization history
g. Insurance card, etc.

Suspicious Personal Identifying Information:

1. Identifying information presented that is inconsistent with other information the customer provides (i.e. inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (i.e. an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (i.e. an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one provided by another customer;
6. Address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (unless by law social security numbers must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

Suspicious Account Activity or Unusual Use of Account:

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (i.e. very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the College that a customer is not receiving mail sent by the College;
6. Notice to the College that an account has unauthorized activity;
7. Breach in the College’s computer system security; and
8. Unauthorized access to or use of customer account information.

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:

1. Monitoring a covered account for evidence of identity theft;

2. Deny access to the covered account until other information is available to eliminate the red flag;

3. Contact the student;

4. Change any passwords, security codes or other security devices that permit access to a covered account;

5. Reopening a covered account with a new account number;

6. Not opening a new covered account;

7. Closing an existing covered account;
8. Notify law enforcement; or
9. Determine no response is warranted under the particular circumstances.

In all situations where it is determined that a Red Flag has been positively identified, the Director/Department Head/Dean shall document the discovery of the Red Flag, the inquiry of the Red Flag, and any specific actions taken to mitigate an actual identity theft discovered. This information should be forwarded to the Program Administrator, Director of Accounting, and Vice Chancellor of Finance for review and documentation of the event.

OVERSIGHT OF THE PROGRAM

The Director of Accounting designates a Finance Office staff member to serve as the Program Administrator. The Program Administrator has the responsibility for developing, implementing and updating this Program. Specifically, the Program Administrator will be responsible for the Program administration; ensuring appropriate training of the College's staff on the Program; 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 NTCC from identity theft. Once per year by July 1, unless otherwise mandated or required, 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 make recommendations to the Vice Chancellor of Finance & Director of Accounting to update the Program.

STAFF TRAINING

NTCC Finance Office 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.

Internal Steps:
NTCC will take the following steps from its internal operating procedures to prevent the likelihood of identity theft occurring with respect to covered accounts:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to covered account information are password protected;
4. Limit the use of social security numbers to activities for which they are required;

5. Ensure computer virus protection is up to date; and

6. Require and retain only student and employee information necessary for College purposes.

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

NTCC 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.

For all service provider arrangements, students will contact the service provider directly via website or telephone and provide personally identifying information to be matched to the records that the College has provided to the service provider.

NON-DISCLOSURE OF SPECIFIC PRACTICES

For the effectiveness of this Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited. The Program Administrator and Academic/Student Services shall disseminate the necessary information to employees with a need to know. Any documentation regarding the development or implementation of this Program that lists or describes specific practices or contains confidential information should not be shared with other College employees or the public. All documents and specific practices related to the Program should be maintained in a confidential manner.

Policy Reference: *LCTCS Identity Theft Prevention Program Policy No.5.028*
Fair and Accurate Credit Transactions Act of 2003

Review Process:

X	Reviewing Council/Entity	Review Date	Effective Date
X	Finance Department	07/11/2017	09/07/2017
X	College Leadership Team	07/11/2017	09/07/2017
X	Chancellor	07/11/2017	09/07/2017
X			

Distribution: Distributed Electronically via College’s Internet
Hard Copy Distribution to NTCC Leadership Team