SECTION: Administrative

SUBJECT: Identity Theft Prevention Program

Background: The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The program must provide for the identification, detection, and response to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

Point of Contact: Vice President for Finance and Administration

Other LCSC offices directly involved with implementation of this policy, or significantly affected by the policy: Controller's Office, Information Technology, Student Services, Student Union Auxiliary, Security

Date of approval by LCSC authority: November 20, 2015

Date of State Board Approval: 6/18/09

Date of Most Recent Review: 6/2019

Summary of Major Changes incorporated in this revision to the policy: Minor change to include additional items to be included in identification of red flags.

Policy:
In accordance with the Fair and Accurate Credit Transactions Act (FACTA) of 2003, the College has established an Identify Theft Prevention Program to identify relevant red flags for new and existing covered accounts, detect new red flags, and respond appropriately to any red flags that are detected.

1. **Definitions:**
   A. **Identity theft**: Fraud committed or attempted using the identifying information of another person without authority.
   B. **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.
   C. **Red Flag**: A pattern, practice or specific activity that indicates the possible existence of identity theft.
   D. **Personally identifying information**: Any name or number that may be used alone or in conjunction with other information to identify a specific person including an individual's name, address, date of birth, social security number, driver's license number, passport number, tax identification number, student identification number, or banking account information.

2. **Identification of Red Flags**

A. In order to identify relevant red flags, the College must analyze the types of accounts it maintains, methods it provides to open and access these accounts and its previous experiences with identity theft. Accordingly, the following red flags have been identified for each of the categories listed:

(1) Suspicious Documents
- (a) Identification document or card that appears to be forged, altered, or unauthentic.
- (b) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.
- (c) Other document with information that is not consistent with existing student information.
- (d) Any application that appears to have been forged or altered.

(2) Suspicious Personal Identifying Information
- (a) Identifying information that is inconsistent with other information the student provides; for example, two documents with different birth dates.
- (b) Identifying information that is inconsistent with other sources of information; for example, supplemental documentation for a student loan with a different address than that on file with the College.
- (c) Identifying information that is the same as information shown on other applications that were found to be fraudulent.
- (d) Identifying information presented that is consistent with fraudulent activity; for example, an invalid phone number or fictitious address.
- (e) Social Security Number that is the same as another student or employee.
- (f) Address or phone number that is the same as another student or employee.
- (g) An individual who fails to provide complete personal identifying information on an application when prompted to do so.

(3) Notifications and Warnings from Credit Reporting Agencies
- (a) Report of fraud accompanying a credit report.
- (b) Notice or report from a credit agency of a credit freeze on an applicant.
- (c) Receipt of a notice of address discrepancy in response to a credit report request.
- (d) Indication from a credit report of activity that is inconsistent with an applicant's usual behavior or activity.

(4) Suspicious Covered Account Activity or Unusual Use of Account
- (a) Change of address for an account followed by a request to change the student's name.
- (b) Payments stop on an otherwise consistently up-to-date account.
- (c) Account is used in a way that is not consistent with prior use.
- (d) Mail sent to a student is consistently returned as "undeliverable".
- (e) A student notifies the College that s/he is not receiving mail sent by the College.
- (f) A student notifies the College that an account has unauthorized activity.
- (g) Unauthorized access to or use of student account information.

(5) Missing or stolen information
- (a) Computers

(b) Computer files, flash drives, etc.
(c) Paperwork with sensitive data, i.e. social security numbers

(6) Alerts from Other Sources
Notice to the College from a student, identity theft victim, law enforcement or other individual that the College has opened or is maintaining a fraudulent account for a person engaged in identity theft.

3. Detecting Red Flags

A. New Covered Account Student Enrollment: In order to detect any of the red flags identified above that are associated with the enrollment of a student, College personnel must take the following steps to obtain and verify the identity of the individual opening the account:
(1) Require certain identifying information such as name, date of birth, academic records, home address or other identifying information; and
(2) Verify the student's identity at the time of issuance of student Warrior ID card via identity confirmation against the student's driver's license or other government issued identification.

B. Existing Student Account Activity: In order to detect any of the red flags identified above for an existing covered account, College personnel must take the following steps to monitor account transaction:
(1) Verify the identity of students requesting information in person, by mail, email or facsimile;
(2) Verify the identity of individuals requesting to change billing addresses by mail or email;
(3) Provide student with a reasonable means of promptly reporting incorrect billing address changes; and
(4) Correspond with student if informed by the bank that banking information given for a one-time payment is incorrect.
(5) Correspond with student if informed by the bank that direct deposit banking information retained by LCSC has changed or become invalid.

C. Consumer Credit Reports: In order to detect red flags identified above for any covered account for which a credit report is required, the College will take the following steps to assist in identifying address discrepancies:
(1) Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency.
(2) In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the report was requested and report to the consumer reporting agency an address for the applicant that the College has taken reasonable steps to confirm is accurate.

4. Preventing and Mitigating Identity Theft

A. Reporting Requirement: In the event that College personnel detect any red flags, one or more of the following steps must be taken, depending on the degree of risk posed by the red flag:
(1) Monitor the identified covered account for evidence of identity theft.

(2) Contact the student or applicant for which a credit report was run, where applicable.
(3) Change any passwords or other security devices that permit access to covered accounts.
(4) Provide the student with a new student identification number.
(5) Notify law enforcement.
(6) Other action as recommended by the Program Administrator.

B. Protecting Student Identifying Information: In order to prevent the likelihood of indentify theft occurring, College personnel will take the following steps with respect to internal operating procedures to protect student identifying information:
(1) Ensure that institutional web pages are secure or provide clear notice where web pages are not or cannot be secured.
(2) Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision had been made to discard that information.

(3) Avoid the use of social security numbers except when required for tax or other governmental reporting purposes.
(4) Maintain up-to-date computer virus protection.
(5) Require and maintain the minimum amount of student information necessary for institutional purposes.

5. Program Administration

A. Oversight: Responsibility for implementing and updating the Identity Theft Prevention Program lies with the Vice President for Finance and Administration.
(1) Staff training will be conducted for those who may come into contact with accounts or personally identifiable information that may pose a risk to the College or its customers.
(2) All employees will complete the cyber-security training mandated by the State of Idaho.
(3) Service Provider Arrangements: In the event the College engages a service provider to perform an activity in connection with one or more covered accounts, the College will take the following steps to ensure the service provider performs its duties in accordance with all institutional policies and procedures designed to detect, prevent and mitigate the risk of identity theft:
(a) Require, by contract, that service providers understand and agree to abide by College policies and procedures regarding identity theft.
(b) Require, by contract, that service providers report any red flags to the College employee with primary oversight of the service provider.
(c) Require, by contract, that service providers report, and correct, any cyber breaches to the College.
(4) Program Updates: The Vice President for Finance and Administration will periodically review and update the Identity Theft Prevention Program to reflect changes in risks. This review will consider the institution’s experiences with identity theft, changes in the means by which identity theft occurs, changes in identity theft prevention and detection methods, and changes in the way business relationships are structured with other entities. After considering these changes, modifications to the program will be instituted as warranted.