Columbus State Community College
Identity Theft Prevention Program
Effective June 1, 2010
Last Updated: February 10, 2016

I. Program Adoption

Pursuant to the Red Flags Rule, issued by the Federal Trade Commission (FTC) under Sections 114 and 315 of the Fair and Accurate Credit Transactions Act, Columbus State Community College ("the College") has developed this Identity Theft Prevention Program (Program). *This program was approved by the Columbus State Community College Board of Trustees on May 27, 2010.*

II. Definitions

1) Identity Theft – fraud committed or attempted using the identifying information of another person without authority.

2) Red Flag – a pattern, practice, or specific activity that indicates the possible existence of identity theft.

3) Covered Account:

   - An account that a financial institution or creditor offers or maintains, primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

   - Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to students or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

4) Program Administrator – the individual designated with primary responsibility for oversight of the program. See Section VI below.

III. Identification of Relevant Red Flags

Common risk factors that will be considered by College personnel to identify relevant red flags for covered accounts includes the following:

1) Receipt of notice of dispute from a credit agency;

2) Identification document or card that appears to be forged, altered or inauthentic;

3) Identification document or card on which a person's photograph or physical description is inconsistent with the person presenting the document;

4) Other document with information that is inconsistent with employee or student information;

5) Identifying information presented that is inconsistent with other information the employee or student provides (e.g., inconsistent birth dates);

6) Identifying information presented that is inconsistent with other sources of information (e.g., an address not matching an address on a loan application or institution's current student record);

7) Social security number presented that is the same as one given by another student, or employee;

8) Notice to the College that an account has unauthorized activity;

9) Notice by student to the College of unauthorized access to or use of student account information;

10) Notice to the College from a student, employee, identity theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in identity theft;

11) Student signs a different name on different college forms;

12) Student presents conflicting demographic information during registration or other student service without presenting a corroborating piece of identification;

13) Student receives a bill and asserts that he/she did not receive services at the College and other processes indicate that this is likely to be true;

14) Student or student's representative admits during any process that someone else's identity is being used.

IV. Detecting Red Flags

College personnel shall detect red flags in connection with the opening of covered accounts and activity related to existing covered accounts by:

1) Obtaining identifying information about a person opening a covered account, and verifying the identity of that person;

2) Authenticating customers, monitoring transactions and verifying the validity of change of address requests in the case of existing covered accounts;

3) Verifying a student's identity at time of issuance of student identification card (e.g., review of driver's license or other government issued photo identification);

4) Verifying the identification of students requesting information (in person, via telephone, via facsimile, via e-mail);

5) Requiring 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 a consumer reporting agency.

V. Preventing and Mitigating Identity Theft

In the event that any red flags are detected, College personnel will respond to prevent or mitigate identity theft by taking one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1) If fraudulent activity is suspected, engage the Information Security Office. The Information Security Office will work with the involved teams and document actions taken for legal purposes.

    a. If the Information Security Office deems the activity to be fraudulent, engage the Columbus State Police Department promptly.

2) Change the existing password to a temporary password.

3) Contact the user, notifying them that their account experienced fraudulent or suspicious activity and, as a safety precaution, CSCC has taken measures to prevent further account activity.

    a. Deny access to the account in question until the user can prove, without a doubt, their identity.

4) Work with the appropriate system administrators to ensure all entrance points to the network are blocked.

VI. Program Administration

1) Oversight

The Vice President of Information Technology is responsible for implementing this Program, and shall engage the Information Security Committee established pursuant to Procedure 15-01(M) as necessary and appropriate to assist with the following responsibilities:

- Ensuring appropriate Program training of College personnel who work with covered accounts;
- Reviewing any reports regarding the detection of Red Flags and the steps taken to prevent and/or mitigate identity theft;
- Assisting in the determination of which steps for prevention and mitigation should be taken in particular circumstances;
- Integrating the Program with other information security programs administered by the College;
- Considering and recommending periodic changes to the Program.

2) Staff Training

Relevant College personnel will be identified and trained, as necessary, to implement the provisions of this Program effectively.

3) 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 procedure 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.

4) Program Updates

The Program will be periodically reviewed and updated to address changing risks of identity theft. In doing so, consideration will be given to the college's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the college's business arrangements with other entities.