COLLEGE of CENTRAL FLORIDA	**COLLEGE of CENTRAL FLORIDA** **ADMINISTRATIVE PROCEDURE**

Title: Identity Theft Prevention Program Procedure	
Page 1 of 5	**Implementing Procedure For Policy # # 2.04**
Date Approved: 07/07/11	**Division: Administration and Finance**

Purpose

This Program is intended to identify third party arrangements and "red flags" that will alert College employees when new or existing billing accounts are opened using false information, protect against the establishment of false student accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events. Within the context of this procedure, "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Scope

This procedure applies to "covered accounts," credit report usage, and third party service arrangements within the Identity Theft Red Flags rule.

1. Scope and General Guidelines

   A. "Covered Accounts" under the Red Flags Rule is a consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly, or multiple payments in arrears, in which a "continuing relationship" is established. Certain payment arrangements, such as payment of tuition in full at the beginning of each semester either by the student's family or through a third-party student loan provider (see also, section 3 "Oversight of Third Party…"), does not meet the "continuing relationship" standard in the "covered account" definition.

   B. The College is considered a "creditor" under the Red Flags Rule because it defers payment for services rendered.

   C. C. The procedure also applies when the College uses consumer reports to conduct background checks on prospective employees (e.g. College Administrators) and students.

2. Responsibilities and Delegation of Authority

This Program is intended to identify red flags that will alert College employees when new or existing billing accounts are opened using false information, protect against the establishment of false student accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

The Vice President is responsible for the oversight of the Program. The Chief Information Officer and the Assistant Vice President, Finance are responsible for an annual review of the Program.

3. Internal Risk Assessment

College of Central Florida will conduct random risk assessments to evaluate how at risk the current procedures are at allowing students to create a fraudulent account and evaluate if current (existing) student accounts are being manipulated. This risk assessment evaluates how new accounts are opened and the methods used to access the account information. This risk assessment also includes third party service arrangements used as part of the hiring process. Using this information the College is able to identify areas of highest risk for review and compliance:

- New accounts opened In Person
- New accounts opened via Web
- Account information accessed In Person
- Account information accessed via Telephone
- Account information accessed via Web Site
- Delinquent accounts placed with an outside collection agency

Oversight of Third Party Service Providers:

The College will, as part of its contracts with third party service providers (for example, collection agencies), require as part of the contract that these providers have policies, procedures and programs that comply with the "Red Flag" Rule. Further, Service providers must notify the College of any security incidents they experience, even if the incidents may not have led to an actual compromise of the College's applicant data.

4. Identifying Red Flags

The College adopts the following "red flags" to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- Fraud or active duty alerts included with consumer reports
- Notice of credit freeze provided by consumer reporting agency
- Notice of address discrepancy provided by consumer reporting agency
- Inconsistent activity patterns indicated by consumer report such as:
    - Recent and significant increase in volume of inquiries
    - Accounts placed on hold for financial delinquency
- Identification documents appear to be altered
- Photo and physical description do not match appearance of applicant
- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file.
- Application appears altered or destroyed and reassembled
- Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
- Lack of correlation between the SS# range and date of birth
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of prior fraudulent activity)
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- SS#, address, or telephone # is the same as that of other applicant at College
- Applicant fails to provide all information requested
- Personal information provided is inconsistent with information on file for applicant
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- Identity theft is reported or discovered

5. Response to Attempted/Suspected Fraudulent Use of Identity

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to their cognizant Administrator and the Chief Information Officer/Assistant Vice President, Finance.

Internal Notification

Any College employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify their cognizant Administrator who will then notify the Chief Information Officer/Assistant Vice President, Finance.

External Notification

Affected Individual – The College will notify the affected individual(s), if possible, of any actual identity theft. The following information will be included in the notice:

- General information about the incident;
- The type of identifying information involved;
- The College telephone number that the affected individual can call for further information and assistance;
- The local Law Enforcement Agency with proper jurisdiction;
- The Federal Trade Commission (FTC) Telephone Number: 877-438-4338 and the FTC ID Theft website: http://www.consumer.gov/idtheft
- Advise affected individual to place fraud alerts on their credit reports by contacting the Credit Reporting Agencies:
    - Equifax: (800) 525-6285 or http://www.equifax.com
    - Experian: (800) 397-3742 or http://www.experian.com
    - TransUnion: (800) 916-8800 or http://www.transunion.com

Method of Contact:

- Written notice: certified mail to last known "good address" if identity theft involves alteration of correct address of record.
- Telephone: provided the contact is made directly with the verified, affected person and appropriately documented.

Local Law Enforcement:

In all cases, the College will notify College Public Safety and Local Law Enforcement having proper jurisdiction of any attempted or actual identity theft.

6. Employee Training

The College will implement periodic training to emphasize the importance of meaningful data security practices and to create a "culture of security." The College acknowledges that a well-trained workforce is the best defense against identity theft and data breaches.

- Annually, explain the Program rules to relevant staff, and train them to spot security vulnerabilities, and update them about new risks and vulnerabilities.
- Inform employees of College's "Appropriate Use Procedure " # 3.25.
- Inform employees of College's "Fraud Procedure" #2.04.
- Inform employees of FERPA Guidelines.
- Advise employees that violation of the College's security policies is grounds for discipline, up to, and including, dismissal.

7. Identity Theft Prevention Program Review and Approval

The Chief Information Officer/Assistant Vice President, Finance will review the program at least annually, or after each and every attempt of identity theft. A report will be prepared annually and submitted to the Vice President to include matters related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

Vice President. Administration & Finance	Date
Approved by President	Date