PROCEDURE

SUBJECT	PROCEDURE: IDENTITY THEFT PREVENTION PROGRAM	PAGE P4.011-1
LEGAL AUTHORITY	P6Hx23-4.011	4/21/09 Revision 09-4

P6Hx23-4.011 PROCEDURE: IDENTITY THEFT PREVENTION PROGRAM

I. Purpose

To establish a procedure for identifying “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. This policy must be consistent with Florida Statutes and State Board of Education Rules and the Fair and Accurate Credit Transactions Act of 2003.

II. 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 or payment plan that is billed or payable on a future date, or multiple payments in arrears, in which a “continuing relationship” is established.

B. The College is considered a “creditor” under the Red Flags Rule because it allows students to register now and pay on a future due date and offers Institutional payment plans to students.

C. The Procedure also applies when the College uses consumer reports to conduct credit or background checks on prospective employees.

III. Responsibilities and Delegation of Authority

A. 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.

B. The vice president of Administrative/Business & Information Services is responsible for the oversight of the Program. The

director of Student Accounting and Business Systems is responsible for the development, implementation, administration, and annual review of the program.

IV. 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.)

- Notice of credit freeze provided by credit reporting agency.
- Notice of address discrepancy provided by consumer reporting agency.
- 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. social security number not issued or listed as deceased).
- Lack of correlation between the social security number range and date of birth.
- Information provided is associated with known fraudulent activity (e.g. address or telephone 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 telephone number associated with answering service/pager).

- Social security number, address, or telephone number 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.

V. Response to Attempted/Suspected Fraudulent Use of Identity

A. Internal Notification

Any College employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identity must notify the campus associate provost, the vice president of Administrative/Business & Information Services, and the director of Student Accounting and Business Systems.

B. External Notification

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

1. General information about the incident;

2. The type of identifying information involved;

3. The College telephone number that the affected individual can call for further information and assistance;

4. The local law enforcement agency with proper jurisdiction;

5. The Federal Trade Commission (FTC) telephone number: 877-438-4338 and the FTC ID Theft website: http://www.consumer.gov/idtheft.

6. 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://transunion.com

C. Method of Contact

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

D. Local Law Enforcement

In all cases, the College will notify the director of Security – Risk Management and Operations and local law enforcement having proper jurisdiction of any attempted or actual identity theft.

VI. Employee Training

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

- Annually explain the program rules to relevant staff and train them to spot security vulnerabilities, as well as update them about new risks and vulnerabilities.

- Train employees of the importance of safeguarding confidential information, FERPA guidelines, and College ethics policies.

- Advise employees that violation of the College's security policies is grounds for discipline up to, and including, dismissal.

VII. Identity Theft Prevention Program Review and Approval

The director of Student Accounting and Business Systems will review the program at least annually, or after each and every attempt at identity theft. A report will be prepared annually and submitted to the vice president of Administrative/Business & Information Services to include matters related to the program, the effectiveness of the policies and procedures, a summary of any identity theft incident(s) and the response to the incident(s), as well as recommendations for substantial changes to the program, if any.

History: To Be Adopted 4/20/09. To Be Effective 4/20/09.