6.3.6.1 Identity Theft Prevention Program

I. Purpose & Scope

The development of this Program was pursuant to the Federal Trade Commission's ("FTC") Red Flag Rules arising from the Fair and Accurate Credit Transactions Act (the "FACT Act"). The College's Program is designed to detect, prevent and mitigate identify theft in connection with the opening of a covered account or any existing covered accounts within the College, and is appropriate to the size and complexity of the College as a creditor and the nature and scope of its activities.

II. The "Red Flag Rules" Overview

As a requirement of the Red Flag Rules, a creditor is to periodically determine, by conducting a risk assessment, whether it offers or maintains covered accounts. Upon identifying any covered account(s), the creditor is required to develop and implement a written Identity Theft Prevention Program designed to:

A. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
B. Detect Red Flags that have been incorporated into the Program;
C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
D. Ensure that the Program is updated periodically to reflect changes in risks to the account holders or to the safety and soundness of the creditor from Identity Theft.

III. Definitions

A. **"Account"** means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. It includes (i) an extension of credit, such as the purchase of property or services involving a deferred payment, and (ii) a deposit account.
B. **"Covered Account"** means (i) 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 and (ii) any other account that the creditor offers to maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
C. **"Identity Theft"** means a fraud committed or attempted using the identifying information of another person without authority.
D. **"Red Flag"** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
E. **"Service Provider"** means a person that provides a service directly to the financial institution or creditor.

IV. Covered Accounts

For the purpose of this Program, covered accounts shall include accounts receivable accounts.

V. Red Flag Identification and Detection

To identify and detect Red Flags, the following actions will be taken, when appropriate given the particular covered account and under the particular circumstances, to confirm the identity of individuals requesting services and to prevent and mitigate Identity Theft:

A. Verify identity of person requesting service utilizing a picture ID or alternative means of identification (e.g. driver's license) and/or by other means of authentication in order to reset online accounts.
B. Examine documentation presented to insure it has not been altered or forged.
C. Observe documentation presented and note inconsistencies with data already available in the Banner database.
D. Examine personal identifying information provided for inconsistencies with information on record.
E. Observe account activity for transactions that are inconsistent with normal patterns.
F. Investigate postal mail that is repeatedly returned as undeliverable even though activity continues on that account.
G. Investigate any notices received regarding unauthorized transactions on the account.
H. Take appropriate steps to modify the applicable process to prevent similar activity in the future.

VI. Program Administration

A. After initial approval by the Board of Trustees, the Executive Vice President is responsible for the implementation and future revisions of the Program.
B. The Program should be periodically reviewed and updated after conducting a risk assessment. This should consider any changes in risks to accounts that might have occurred since the last assessment.
C. While each red flag occurrence would not necessarily be a case of identity theft, each case should be examined carefully to determine the level of risk. Any occurrence determined to be high risk should be reported to the Executive Vice President. The Executive Vice President in consultation with others will make a determination for appropriate corrective action.
D. Training programs to effectively train staff in the identification, detection, prevention and mitigation of red flag occurrences should be developed and monitored.
E. In cases where the college utilizes service providers, steps should be taken to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.