**LAKE-SUMTER STATE COLLEGE**
**ADMINISTRATIVE PROCEDURES**

TITLE: IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULES) NUMBER: PRO 6-32

REFERENCE: Rule 2.24
Fair and Accurate Credit Transactions Act
of 2003 Florida Statute 1001.61, 1001.63 & 1001.64
Florida Administration Code SBE 6A-14.0261



## I. PROGRAM ADOPTION

Lake-Sumter State College developed this Identity Theft Prevention Program ("Program") in accordance with the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

## II. BACKGROUND

In 2003, the U.S. Congress passed the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), which amended the Fair Credit Reporting Act ("FCRA") by requiring the FTC and several other federal agencies to issue regulations requiring financial institutions and other "creditors" to adopt policies and procedures to prevent identity theft. In 2007, the FTC, in conjunction with several other federal agencies issued the regulations required under FACT Act, known as the Red Flags Rule.

## III. PURPOSE AND SCOPE

The purpose of this Program is to ensure that the College complies with the Red Flags Rule regulations. The Program was designed with the goal of identifying, detecting, preventing and mitigating identity theft against the College, its faculty, staff, students, constituents and third-party service providers with whom the College contracts to perform certain functions on its behalf. As such, this policy outlines the required Red Flags Rule Program of Lake-Sumter State College, but it is also a comprehensive document which includes not just financial or credit accounts, but any account, process, or database for which the College believes there is a reasonably foreseeable risk to the College, its students, faculty, staff, or constituents from identity theft. Any time an employee suspects a fraud involving personal information about an individual or individuals, the employee should act as if this Identity Theft Program applies and follow protocols established by his/her office for investigating, reporting and mitigating identity theft. The College on a broader scale will take a close look at all databases and software used and develop a plan to ensure all systems are accounted for, protected from security breach and identity theft.

a. Definitions
   1. Covered Account - an account that a financial institution or creditor maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. For the purposes of the College's Identity Theft Program, the term covered account is extended to include any College account or database (financial and non-financial based) for which the College believes there is a reasonably foreseeable risk to the College, its students, faculty, staff, constituents or customers from identity theft;
   2. Creditor - includes any entity who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. The College is considered a "creditor" because it offers student deferments, bills for tuition and fees, and for other provided goods and services (space rental, performances, etc.);
   3. Identifying Information - any name or number that may be used, alone or in conjunction with any other information, to identity a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employee or taxpayer identification number, unique electronic identification number, or computer's Internet Protocol address or routing code;
   4. Identity Theft - means that a fraud was attempted or committed using the identifying information of another person without his/her permission;
   5. Red Flag - a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

b. Identification and Detection of Red Flags.

   The following Red Flags are potential indicators or warning signs of potential or actual identity theft or similar fraud. Any time a Red Flag, or a situation resembling a Red Flag, is apparent, it must be investigated for verification. As an appendix to the Red Flags Rule, the FTC has identified twenty- six Red Flags that the College may consider incorporating into its identity theft program. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary. These Red Flags are subdivided into five sections below:
   1. Alerts. Notifications or Warnings from a Consumer Reporting Agency.
      i. A fraud or active duty alert is included with a consumer report;
      ii. A notice of credit freeze on a consumer report;
      iii. A consumer reporting agency provides a notice of address discrepancy;
      iv. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of customer.
   2. Suspicious Documents
      i. Documents provided for identification appear to have been altered or forged;
      ii. The photograph or physical description on the identification is not consistent with the appearance of the customer presenting the identification;
      iii. Other information on the identification is not consistent with information provided by the person opening an account or presenting the identification;

iv. Other information on the identification is not consistent with readily accessible information that is on file with the College;
v. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

3. Suspicious Personal Identifying Information
   i. Personal identifying information provided is inconsistent when compared against external information sources used by the College;
   ii. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer;
   iii. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College;
   iv. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College;
   v. The social security number provided is the same as that submitted by other persons opening an account or other customers;
   vi. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers;
   vii. The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;
   viii. Personal identifying information provided is not consistent with personal identifying information that is on file with the College;
   ix. If the College uses a challenge question, the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
4. Suspicious Account Activity or Unusual Use of Account
   i. Shortly following the notice of a change of address for a covered account, the College receives a request for a new, additional, or replacement card, or for the addition of authorized users on the account;
   ii. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns;
   iii. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
   iv. An account that has been inactive for a reasonable period of time is used. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account;
   v. The College is notified that the customer is not receiving paper account statements;
   vi. The College is notified of unauthorized charges or transactions in connection with a customer's account.

5. Alerts from Others

   Notice to the College by a student/customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

c. College-Wide Response to Detected Red Flags

Once potentially fraudulent activity is detected, an employee must act immediately as a quick appropriate response can protect customers and the College from the effects of identity theft.

Appropriate Actions examples may include, but are not limited to:

1. Canceling the transaction;
2. Notifying and cooperating with appropriate law enforcement;
3. Notifying the Senior Administration of the College who will notify the College Attorney; and/or
4. Notifying the actual student/customer that fraud has been attempted or that it has occurred;
5. Changing any passwords or other security devices that permit access to relevant accounts and/or databases; and/or
6. Continuing to monitor the account or database for evidence of identity theft;
7. Alternatively, it may be determined that no response is warranted after appropriate evaluation and consideration of the particular circumstances.

Response to Attempted/Suspected Fraudulent Use of Identity

1. Internal Notification: Any College employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must inform his/her Department Head as soon as possible that he/she has detected an actual or potential Red Flag, or has identified a similar area of concern of identity theft. The Department Head will conduct any necessary inquiries to determine the validity of the Red Flag. If it is determined that a situation of identity theft has occurred, the Department Head will ensure that appropriate actions are taken to immediately mitigate the harm done and in doing so, he/she will inform the Senior Administration of the College for further recommendation on the handling of the matter so it is properly documented as part of the monitoring portion of the College's Program. Appropriate actions will be dependent on the type of Red Flag identified, type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and numerous other factors;
2. 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:
   i. General information about the incident;
   ii. The type of identifying information involved;
   iii. The College telephone number that the affected individual can call for further information and assistance;
   iv. The local Law Enforcement Agency with proper jurisdiction;

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

vi. 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.

3. Method of Contact: Written notice sent certified mail to last known "good address" if identity theft involves alteration of correct address of record. Telephone individual provided the contact is made directly with the verified, affected person and appropriately documented;
4. Local Law Enforcement: In all cases, the College will notify the Executive Vice President who will notify Local Law Enforcement having proper jurisdiction of any attempted or actual identity theft. Document all situations where it is determined that a Red Flag has been positively identified. The Department(s) responsible for the account will document what occurred, describe the matter and any specific actions taken to mitigate the impact of the effects of the actual or potential identity theft discovered. The documentation will also include a description of any additional actions the department believes are systemically necessary (such as updating policies and procedures) in response to identified Red Flag to handle or prevent similar situations in the future. This report shall be sent to the Senior Vice-President of Business Affairs for inclusion in his report to the President.

d. Consumer "Credit" Report Requests and Verification

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is necessary, 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 request was made and repost to the consumer reporting agency an address for the applicant that the College has reasonably confirmed is accurate;
3. Review its own records (e.g., job applications, change of address notification forms, other customer account records) to verify the address of the applicant;
4. Verify the address through third-party sources with whom the College is currently contracted.

e. Employee Training

Staff training is required for all employees for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the College and/or its students or employees. The Professional Development Center - is responsible for ensuring that appropriate identity theft training and a copy of the Program is provided to all employees during new employee orientation and others as appropriate at least annually. The Identity Theft training for all staff members will help them identify Red Flags, and provide guidance on what to do in the event he/she detects a Red Flag or have similar concerns regarding an actual or potential fraud involving personal information.

Annual training provided through the PDC -will 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.

1. Annually, explain the Program rules to relevant staff, and train them to spot security vulnerabilities, and update them about new risks and vulnerabilities;
2. Inform employees of College" Identity Theft Prevention Program (Red Flag Rules)" PRO 6-32;
3. Inform employees of College's Code of Ethical Behavior Rule 1.10 and Fraud Reporting Procedure 6-30;
4. Inform employees of FERPA Guidelines;
5. Advise employees that violation of the College's security policies are grounds for discipline, up to, and including, dismissal (Rule 2.17 and Procedure 2-12).

f. Third Party Service Providers Agreements

When the College engages a third-party 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 all activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risks of identity theft.

Lake-Sumter State College will require the service provider to do the following:

1. Require, by contract, that the service provider(s) have such policies and procedures in place; and
2. Require, by contract, that the service provider is
    i. aware of and reviews the College's Identity Theft Program; and
    ii. reports any identified Red Flag as soon as possible to the Senior Administrators of the College or the College employee with primary oversight of the service provider relationship.

g. Program Administration

Responsibility for the implementation of the Identity Theft Program ultimately rests on each department at the College, the employees of each department that maintains accounts or databases covered by this Program, and the College Community as a whole. As permitted by the Red Flags Rule regulations, responsibility for overseeing the administration of the Program has been delegated to the Executive Vice President and Chief Information Officer with annual compliance monitoring responsibility to be performed by the Identification Security Task Force (IDSTF).

The IDSTF will be a cross-functional group of College personnel tasked with coordination of the administration, reporting, and modification of this procedure. The IDSTF will meet regularly to implement these procedures. The IDSTF shall, at a minimum, consist of key personnel from Student Registration, Financial Aid, Business Services, Academic Admissions, Information Technology, Human Resources and Security.

h. Program Updates

The IDSTF will periodically review and recommend updates to reflect changes in risks to students, employees, technological changes and the soundness of the Program. This review will include the College's experiences with Identity Theft situations, changes in Identity Theft detection and prevention methods, business arrangements with third-party service providers, an assessment of which accounts, activities and/or databases are covered by the Program and to re-evaluate employee training.

NEW: 01/07/2014