LOUISIANA COMMUNITY & TECHNICAL COLLEGE SYSTEM
Policy # 5.028

Title: IDENTITY THEFT PREVENTION PROGRAM

Authority: Board Action	Original Adoption:	02/11/2009
	Effective Date:	02/11/2009
	Last Revision:	Initial

LCTCS has determined that its institutions fall under the provisions of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Public Law 108-59; specifically, sections 114 and 315. To ensure compliance with the Act, institutions under the auspices of the LCTCS shall develop and implement an appropriate policy and identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account as defined in the Act. (*See Definitions*)

Entities Affected

Louisiana Community & Technical College System (LCTCS) Colleges and Regions.

Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account and to provide for the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the program is updated periodically to reflect changes in risks to students and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions

Identity theft means fraud committed or attempted using the identifying information of another person without authority.

A *covered account* is defined as 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.

A *red flag* is a pattern, practice, or special activity that indicates the possible existence of identity theft.

Covered Accounts

LCTCS College or Regional officials shall identify covered accounts for inclusion in a college or regional Identity Theft Prevention policy. The policy must address covered accounts administered by each college or region and any that are administered by a service provider.

Identification of Relevant Red Flags

LCTCS college or regional officials LCTCS shall identify the relevant red flags for covered accounts. The red flags generally fall into the five categories listed below:

1. Alerts, notifications, or warnings from a consumer reporting agency;
2. Suspicious documents;
3. Suspicious personally identifying information, such as suspicious address;
4. Unusual use of – or suspicious activity relating to – a covered account; and
5. Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the Chancellor or Regional Director of each college or region. The Chancellor or Regional Director's designee will be responsible for the Program administration, for ensuring appropriate training of the college's staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program. The designated official at each college or region is also responsible for sending the policy to the LCTCS Sr. Vice President for Finance and Administration for review and filing.

System Guidance

The System Office has developed a sample policy template for use by each college or region in design of an Identity Theft Prevention Policy. This sample is attached to this policy as a reference

Louisiana Community and Technical System
Name of College or Region:_____
Identity Theft Prevention Program
Sample
{insert name of college or region where indicated)

(College or region should customize text where indicated in bold/italics}

Program Adoption

Louisiana Community and Technical System ("System") developed this identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This program was developed with oversight and approval of the System Office. After consideration of the size of the System's operations and account systems, and the nature and scope of the System's activities, the Board of Supervisors determined that this Program was appropriate for the System, and therefore approved this Program on Mo___Date__Year____

Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to Students and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

A covered account means 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.

A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Covered Accounts

The *(College or Region)* has identified five types of accounts, four of which are covered accounts administered by the System and one type of account that is administered by a service provider.

(College or Region) covered accounts:

1. Refund of credit balances involving PLUS loans
2. Refund of credit balances, without PLUS loans
3. Deferment of tuition payments
4. Emergency loans

Service provider covered account:

1. Tuition payment plan administered by ECSI, refer to "Oversight of Service Provider Arrangements" on page 6.

Identification of Relevant Red Flags

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above;
2. The methods provided to open covered accounts-- acceptance to the *(College or Region)* and enrollment in classes requires the all of the following information:
    a. Common application with personally identifying information
    b. high school transcript
    c. official ACT or SAT scores
    d. two letters of recommendation
    e. Entrance Medical Record
    f. Medical history
    g. immunization history
    h. insurance card
3. The methods provided to access covered accounts:
    a) Disbursement obtained in person require picture identification
    b) Disbursements obtained by mail can only he mailed to an address on file
4. The (College or Region's) previous history of identity theft.

The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request made from a non- (*College or Region)* issued E-mail account;
4. A request to mail something to an address not listed on file; and
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Detection of Red Flags

The Program will detect red flags relevant to each type of covered account as follows:

1. Refund of a credit balance involving a PLUS loan – As directed by federal regulation (U.S. Department of Education) these balance are required to be refunded in the parent's name and mailed to their address on file within the time period specified. No request is required. Red Flag-none as this is initiated by the (College or Region).
2. Refund of credit balance, no PLUS loan - requests from current students must be made in person by presenting a picture ID or in writing from the student's (College or Region) issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing picture ID. Requests from students not currently enrolled or graduated from the (College or Region) must be made in writing. Red Flag-Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
3. Deferment of tuition payment - requests are made in person only and require the student's signature. Red Flag - none.
4. Emergency loan - Requests must be made in person by presenting a picture ID or in writing from the student's (College or Region) issued e-mail account. The loan check can only be mailed to an address on file or picked up in person by showing picture ID. Red Flag – Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
5. Tuition payment plan - Students must contact an outside service provider and provide personally identifying information to them. Red Flag-none, see Oversight of Service Provider Arrangements.

Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the *Designated Officer:* _____ will be responsible for the Program administration, for ensuring appropriate training of *(College or Region)*' *s* staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating

Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

Updating the Program

This Program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the *(College or Region)* from identity theft. *At least once per year in October, the Program Administrator* will consider the *(College or Region's)* experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the *(College or Region)* maintains and changes in the *(College or Region*)'s business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program.

Staff Training

(College or Region) staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

Oversight of Service Provider Arrangements

The *(College or Region)* shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures 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.

Currently the (College or Region) uses ECSI to administer the Tuition Payment Plan and the Perkins Loan. Students contact ECSI directly through its website or by telephone and provide personally identifying information to be matched to the records that the (College or Region) has provided to ESCI.