

POLICIES AND PROCEDURES

Subject: Identity Theft Prevention Program Reference: E-XXVIII-f

Source: Board of Trustees Eff. Date: November 27, 2012

Approval Auth: Board of Trustees Approved: _____

Remarks: _____

Date: November 27, 2012

Program Adoption

McLennan Community College ("MCC") developed the Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule, which implements Sections 114 of the Fair Accurate Credit Transactions Act of 2003. After consideration of the size of the College's operations and account systems, and the nature and scope of the College's activities, the Board of Trustees determined that this Program was appropriate for McLennan Community College, and therefore, the administration presented the Program for approval at the scheduled August 4, 2009 Board Meeting with the program effective as of August 1, 2009.

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, faculty, and staff 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.

Red flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Covered Account means a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition and fee installment payment plan.

Covered Accounts

McLennan Community College has identified four types of accounts which are covered accounts administered by the College.
College covered accounts:

1. Student tuition and fee payment plans
2. Student ID (debit) card accounts in the bookstore
3. Payment of faculty and staff computer purchases through payroll deduction
4. Offering institutional loans to students

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. Methods provided to open covered accounts which require acceptance to the College and enrollment in classes requires the following information:

- a. Common applications with personally identifying information
 - b. High school and college transcripts
 - c. Official test scores
 - d. Medical history
 - e. Immunization history
3. The methods provided to access covered account:
- a. Disbursement obtained in person require picture identification
 - b. Disbursements obtained by mail can only be mailed to an address on file
4. The College's previous history of identity theft.

The Program identifies the following red flags:

1. Documents where the photo ID does not resemble its owner or an application which appears to have been cut up, re-assembled and photocopied.
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 issued e-mail account.
4. A request made to mail something to an address not listed on file.
5. Unusual use or suspicious account activity showing material changes in payment patterns, notification that the account holder is not receiving a mailed statement, or that the account has unauthorized charges.
6. Notice from a victim of identity theft, law enforcement, or other persons regarding possible identity theft in connection with covered accounts.

Detection of Red Flags

Employees shall undertake reasonable diligence to identify red flags in connection with the opening of covered accounts as well as existing covered accounts through such methods as:

1. Obtaining and verifying identity
2. Authenticating customers
3. Monitoring transactions
4. Verifying validity of address changes

Appropriate Responses to Red Flags

The detection of a red flag by an employee shall be immediately reported to the appropriate administrator and based on the type of red flag, the administrator and chief security officer will determine the appropriate response. The administrator will investigate the threat of identity theft to determine if a breach has occurred and will respond appropriately to prevent future identity theft breaches. Upon review of the incident, the responsible administrator and chief security officer shall determine what steps may be required to mitigate any issues that arise in the review. In addition, referral to law enforcement may be required. The following actions will be used in response to Red Flags;

1. Monitoring affected accounts
2. Denying access to the covered account
3. Contacting the student or affected person
4. Changing passwords
5. Providing a new student identification number
6. Notifying the appropriate administrator
7. Notifying law enforcement
8. Determining that no response is warranted under the circumstances

Periodic Updating of the Program

This program will be reviewed on or about the first day of each fiscal year by a committee consisting of individuals from departments affected by the Program. The review will determine whether all aspects of the Program are up to date and applicable in the current business environments, and revised as necessary. The review will also look at the soundness of the Program in

detecting identity theft. It will take into consideration the college's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the college's third party arrangements. After consideration of these factors, the committee will determine whether changes in the Program are warranted and the Program will be updated and presented to the Board for approval of the changes.

Oversight of the Program

Oversight of the Program by the Director of Administrative Services includes:

1. Providing reports to the Board annually of identity theft occurrences
2. Reviewing third party vendor arrangements
3. Assessing the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with covered accounts
4. Recommending material changes needed in the Program

Oversight of the Program by the Board involves:

1. Reviewing reports of identity theft occurrences
2. Approving material changes in the Programs