Southwest Texas Junior College

Identity Theft Program

Approved on xxxxxxxx, 2011

Southwest Texas Junior College
Identity Theft Program

Program Adoption

Southwest Texas Junior College ("College") established the Identity Theft Prevention Program ("Program") in response to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Under the Red Flags Regulations, implementation and oversight of the Identity Theft Program is the responsibility of the governing body or an appropriate committee of such governing body. Approval of the initial plan must be appropriately documented and maintained. After its initial approval of the Program, however, the governing body may delegate its responsibility to implement and oversee the Identity Theft Program.

After consideration of the College's operations and accounts and the nature and scope of the College's activities, the Southwest Texas Junior College Board of Trustees determined that this Program was appropriate for the College and therefore approved this Program on …………………..

Having made such initial approval, the Board of Trustees hereby delegates the responsibility for implementing, monitoring, and overseeing the College's Identity Theft Program to the Human Resources Coordinator to serve as Program Administrator.

Purpose

The Red Flags Rule regulations require entities with accounts covered by those regulations, including colleges, to develop and implement a written Identity Theft Prevention Program (hereinafter, the "Program" or the "Identity Theft Program") for combating identity theft in connection with certain accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable the entity with covered accounts to:

- Identify relevant patterns, practices, and activities, dubbed "Red Flags," signaling possible identity theft and incorporate those Red Flags into the Program;

- Detect Red Flags;

- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and

- Ensure the program is updated periodically to reflect changes in risks.

Definitions

Account: "Account" means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. Account includes:

- An extension of credit, such as the purchase of property or services involving a deferred payment; and
- A deposit account

Covered account:

- A consumer account offered or maintained by the College that involves or is designed to permit multiple payments or transactions, such as a loan or account that is billed or payable in installments;
- An account offered or maintained by the College for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College from identity theft, including financial, operational, compliance, reputation, or litigation risks. For the purposes of the College's Identity Theft Program, the term "covered account" is extended to include any College account or database (financially based or otherwise).

Credit: "Credit" means "the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer their payment or to purchase property or services and defer payment therefore."

Creditor: "Creditor" means "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."

Financial Institution: "Financial institution" means "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer."

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

Program Administrator: "Program Administrator" is the individual designated with primary responsibility for oversight of the Program.

Red Flag: "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Service Provider: "Service provider" means "a person that provides a service directly to the financial institution or creditor."

Identification of Red Flags

A “Red Flag” is a pattern, practice, or specific activity that indicates the possible existence of identity theft. 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 should be investigated for verification. The examples below are meant to be illustrative. Any time an employee suspects fraud involving personal information about an individual or individuals, the employee should assume that this Identity Theft Program applies and follow protocols established by his/her office for investigating, reporting and mitigating identity theft.

Suspicious Documents

- Identification documents or card that appears to be forged, altered or inauthentic
- Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document
- Other document with information that is not consistent with existing student information
- Application for service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled

Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the person provides (example: inconsistent birth dates)
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application)
- Identifying information presented that is the same as information shown on other application that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity such as an invalid phone number or fictitious billing address
- Social security number presented that is the same as one given by another person
- An address or phone number presented that is the same as one given by another person
- A person who fails to provide complete personal identifying information on an application when reminded to do so
- A person’s identifying information that is not consistent with the information that is on file for the individual
- The person or customer opening the covered account cannot provide authenticating information

Suspicious Covered Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the person's name
- Previously up-to-date account suddenly stops receiving payments
- Account used in a way that is not consistent with prior use
- Mail sent to the student is repeatedly returned as undeliverable
- Notice to the College that a student is not receiving mail sent by the College
- Notice to the College that an account has unauthorized activity
- Breach in the College's computer system security
- Unauthorized access to or use of student or employee account information

Alerts from Others

- Notice to the College from a student, Identity Theft victim, law enforcement, or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft

Detection of Red Flags

Student Enrollment

- Require certain identifying information such as name, date of birth, academic records, home address or other identification
- Verify the student's or employee's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification)

Existing Accounts

- Verify the identification of a person if they request information (in person, via telephone, via facsimile, via email)
- Verify the validity of requests to change billing addresses by mail or email and provide the person a reasonable means of promptly reporting incorrect billing address changes
- Verify changes in banking information given for billing, payroll, and payment purposes

Employment Background Checks

- Require written verification from an applicant that the address provided by the applicant is accurate at the time of the request
- In the event that notice of an address discrepancy is received, verify that the background check pertains to the applicant for whom the requested report was made

Responding to detected Red Flags

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the College from the effects of identity theft. The employee should inform his/her supervisor 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 supervisor should conduct any necessary inquiry to determine the validity of the Red Flag. If the Red Flag indicates that a fraudulent transaction has occurred, the department should ensure that appropriate actions to mitigate the effects of the transaction are taken immediately. 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. However, by way of example, appropriate actions may include, but are not limited to:

Prevent and Mitigate

- Continue to monitor a Covered Account for evidence of Identity Theft
- Change any passwords or other security devices that permit access to Covered Accounts or student information system by contacting IT.
- Do not open a new Covered Account
- Notify the Program Administrator for determination of the appropriate step(s) to take
- Notify and cooperate with appropriate law enforcement
- Consider any aggravating factors that might heighten the risk of identity theft, such as data security breach
- Provide students information on identity theft during New Student Orientation
- Do not share usernames and passwords
- Provide a link on the SWTJC website with information about identity theft, safety, contact information
- File or assist in filing an SWTJC Suspicious Activities Report (SSAR)
- Determine that no response is warranted under the particular circumstances

Protect Student Identifying Information

- Ensure that its website is secure or provide clear notice that the website is not secure
- Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information
- Ensure that office computers with access to Covered Account information are password protected
- Avoid, if possible, using social security numbers
- Ensure computer virus protection is up to date

Program Administration

Administration of the program, including oversight, development, implementation, training, and review is the responsibility of a committee appointed by and reporting to the Program Administrator. This Committee will review reports prepared by staff (at least annually) regarding compliance by the College with applicable federal regulations. The Program (including the Red Flags determined to be relevant) will be updated periodically to reflect changes in risks to customers or to the safety and soundness of the College from identity theft. The Program Administrator will approve material changes to the Program as necessary to address changing identity theft risks.

Successful implementation of the Identity Theft Program ultimately is the responsibility of each office, the employees of each office that maintains accounts or databases covered by this Program, and the College community as a whole.

Committee Members

Admissions/Registrar's Office
Bookstore
Business Office
Campus Police
Financial Aid Office
IT Department

Staff Training

All employees who process information related to covered accounts shall receive training following appointment on the procedures outlined in this document. Additional training may be available periodically.

Updating the Program

On an annual basis, the Program Administrator will confer with the College's offices that maintain covered accounts under the Program. The Committee will review each office's list of covered accounts, training and policies, procedures and practices as they relate to preventing, detecting, and mitigating identity theft, and any positively identified Red Flags or similar incidents documented by the offices that maintain covered accounts under this Program.

Each year the Committee will create an annual report, assessing the effectiveness of the College's Identity Theft Program as a whole. As part of the report, the Committee will make recommendations for updating or modifying the Program as appropriate. The annual report will be provided to the Controller for review.

SWTJC Suspicious Activity Report

Always Complete Entire Report

Part One Reporting Institutional Information

□ Check box if you are correcting a prior report.

Southwest Texas Junior College
Name of person filing report:

Date of report: ______________________
Department/Office: ______________________

Account numbers affected (if any)

______________________ ______________________

______________________ ______________________

Part Two Suspect Information

□ Suspect Information Unavailable

Last Name or Name of Entity	First Name		Middle Initial
Address			SSN
City	State	Zip	Date of Birth
Phone Number □ Home □ Cell □ Work		Phone Number □ Home □ Cell □ Work	

Occupation/Type of Business

Forms of Identification of Suspect

□ Driver's License □ SWTJC ID □ Other:

Relationship to SWTJC

Student □ Employee □ Customer □

Part Three Suspicious Activity Information

Admission/Confession □ Yes □ No *Please describe below:*

Date or date range of suspicious activity From: To:	Total dollar amount involved in activity

Summary of characterization of suspicious activity:

□ Identity Theft
□ Check Fraud
□ Credit/Debit Card Fraud
□ Misrepresentation of self
□ Computer Intrusion
□ Counterfeit Item
□ Other: ______________________

Part Four Contact for Assistance

Last Name or Name of Entity	First Name	Middle Initial
Title/Occupation	Phone Number	Date Prepared