IDENTITY THEFT PREVENTION PROGRAM

POLICY

Sherman College developed this Identity Theft Prevention Program (hereinafter Program) pursuant to the Federal Trade Commission's Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003. This program was developed with the approval of the Finance and Audit Committee of the Board of Trustees. The nature and scope of the college's activities relating to operations and accounts were considered to determine this Program.

The purpose of this policy is to establish a Program designed to detect, prevent and mitigate identity theft in connection with Covered Accounts and to provide for continued administration and support of the Program. The required elements of the Program include the ability to:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft 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.
4. Ensure the Program is updated periodically to reflect changes in risks from identity theft.

Definitions

I. Covered Account – Student accounts or loans which are administered by the college that involve or are designed to permit multiple payments or transactions.
II. Identifying Information – Any name or number which may be used alone or in conjunction with other information to identify a specific person including name, address, phone number, social security number, student identification number, birth date, personal email account, governmental issued driver's license or identification number, taxpayer identification, alien registration or passport numbers.
III. Identity Theft – A fraud committed or attempted using the identifying information of another person without authority.
IV. Program Administrator – Person designated to manage the Identity Theft Prevention Program.
V. Red Flag – A pattern, practice or specific activity that indicates the possible existence of identity theft.

Identification of Red Flags

To identify relevant Red Flags, the college considers the types of accounts that it offers and maintains, methods it provides to open its accounts, the methods it provides to access its

accounts and its previous experiences with Identity Theft. The following are relevant Red Flags and examples signaling possible identity theft:

A. Notification and Warnings from Credit Reporting Agencies

a. Report of fraud accompanying a credit report.
b. Notice or report from a credit agency of a credit freeze on a student or applicant.
c. Notice or report from a credit agency of an active-duty alert for an applicant.
d. Indication from a credit report of activity that is inconsistent with a student's usual pattern or activity.

B. Suspicious Documents

a. Identification document or card that appears to be forged, altered or inauthentic.
b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.
c. Other documents with information that are not consistent with existing student information (such as if a person's signature on a check appears forged).
d. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

a. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates).
b. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report).
c. Identifying information presented is the same as information shown on other applications that were found to be fraudulent.
d. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).
e. The social security number presented is the same as one given by another student.
f. The address or phone number presented is the same as that of another person.
g. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required).
h. A person's identifying information is not consistent with the information that is on file for the student.

D. Suspicious Account Activity or Unusual Use of Account

a. Change of address for an account followed by a request to change the account holder's name.
b. Payments stop on an otherwise consistently up-to-date account.
c. Account used in a way that is not consistent with prior use (example: very high activity).

d. Mail sent to the account holder is repeatedly returned as undeliverable.
e. Notice to the college that a student is not receiving mail sent by the college.
f. Notice to the college that an account has unauthorized activity.
g. Breach in the college's computer system security.
h. Unauthorized access to or use of student account information.

E. Alerts from Others

a. Notice to the college from a student, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detecting Red Flags

The Red Flag detection practices are described below.

A. New Accounts – College employees will take the following steps to obtain and verify the identity of the new student.

a. Require certain identifying information such as name, date of birth, home address, academic records or other identification.
b. Verify the student's identity (review license or government issued photo identification).

B. Existing Accounts – College employees will take the following steps to obtain and verify the identity of the person accessing the existing Covered Account.

a. Verify the identification of a student if they request information (in person, via phone, via facsimile, via email).
b. Verify the validity of request to change billing addresses by mail or email.
c. Verify changes in banking information given for billing and payment purposes.

C. Consumer Credit Report Requests – In order to detect any of the Red Flags identified above for an employment position for which a credit or background report is sought, college personnel will take the following steps to assist in identifying address discrepancies:

a. 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.
b. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the college has reasonably confirmed is accurate.

Responding to Red Flags and Mitigating Identity Theft

In the event college staff detects any identified Red Flags, any of the following responses shall be taken to respond and mitigate the identity theft, depending on the situation:

- Continue to monitor an account for evidence of Identity Theft.
- Contact the student.
- Change any passwords, or other security devices that permit access to a covered account.
- Do not open a new account.
- Close an existing account.
- Reopen an account with a new number.
- Report to local authorities (Note: this step shall be taken in all circumstances).
- Notify the Program Administrator.
- Determine no response is warranted under the particular circumstances.

Ensuring the Program is Administered and Updated Properly

A. Staff Training and Reporting

a. College employees 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.
b. Appropriate staff shall provide reports to the Program Administrator on incidents of identity theft, the effectiveness of the Program and the college's compliance with the Program. The reports should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with Covered Accounts, service provider arrangements, significant incidents involving identity theft and the college's response and recommendations for changes to the Program.

B. Service Provider Agreements

a. The college 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 for the college's Covered Accounts.
b. Currently, Sherman College uses ECSI to administer the college's Perkins Loans and payment plans. If an account is administered by ECSI, and is deemed uncollectible through current procedures, the account is turned over to Williams & Fudge collection agency. Data privacy information related to ECSI can be viewed by clicking this link. Data privacy information related to Williams & Fudge can be viewed by clicking this link.