[Reviewed with no changes: August 19, 2015]

Angelo State University
Operating Policy and Procedure

OP 62.03: Red Flag Rules

DATE: August 19, 2015

PURPOSE: The purpose of this Operating Policy/Procedure (OP) is to establish an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flag Rules, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

REVIEW: This OP will be reviewed in July every three years, or as needed, by the Bursar and Information Technology (IT) Security with recommended revisions forwarded through the vice president for finance and administration to the president by August 15.

POLICY/PROCEDURE

1. Definitions

a. Covered Accounts - An account that a creditor offers or maintains for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

b. Creditor - Any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

c. Identity Theft - Fraud committed or attempted using the identifying information of another person without authorization.

d. Personally Identifiable Information - Personally Identifiable Information (PII) is any piece of information, which may be used to uniquely identify, contact, or locate an individual. This PII includes, but is not limited to, taxpayer identification numbers, driver's license numbers, passport identification numbers, passwords, PINs, personal account numbers, computer accounts and passwords, protected health information, financial information, unpublished home addresses or phone numbers, and/or any combination of information that will uniquely identify an individual.

e. Red Flag - A pattern, practice, or specific activity that indicates the possible existence of identity theft.

[Reviewed with no changes: August 19, 2015]

2. General Policy

a. Angelo State University recognizes that some activities of the university are subject to the provisions of the Fair and Accurate Credit Transactions Act (FACT Act) 16 CFR § 681. Per the Federal Trade Commission (FTC) definition, this activity could include participation in the Federal Perkins Loan or Federal Family Education Loan programs, as well as institutional loans to faculty, staff, or students, and tuition payment plans. While Angelo State University may not participate in all these activities, the university strives to protect all PII and prevent identity theft, as required by the FTC Red Flag Rules.

b. As required by the Red Flag Rules, the Identity Theft Prevention Program ("Program") shall include procedures for:

(1) Identifying relevant red flags for new and existing covered accounts,

(2) Detecting red flags that have been incorporated into the Program, and

(3) Responding appropriately to detected red flags in order to prevent and mitigate identity theft.

c. The Program will be periodically updated to reflect environmental, institutional, and legal changes.

3. Authority and Responsibility

a. The controller is designated as the program administrator and will exercise appropriate and effective Program oversight. The program administrator will work with the departmental or unit administrators in areas impacted by the Red Flag Rules. (See Appendix A for a list of these areas.)

b. The program administrator shall conduct an annual Program assessment and provide a report to the vice president for finance and administration, to include recommended Program changes.

c. Each department is responsible for:

(1) Developing, implementing, assessing, and updating the Program;

(2) Developing and maintaining a training program; and

(3) Ensuring compliance of university staff.

d. The program administrator is responsible for reviewing any red flag detection reports and initiating the appropriate response actions.

e. Third party vendors who process any payments for or on behalf of the university must provide documentation certifying their compliance with the FTC's Red Flag Rules.

f. In the event university personnel detect any identified red flags or related suspicious activity, such personnel shall report it immediately to the program administrator, who will conduct further investigation and initiate the appropriate response actions.

Additionally, in accordance with the IT Security Policies and Texas Administrative Code, electronic breaches, regardless of the data type, must be reported to the IT Security Officer. Response to electronic breaches will be in line with the Security Incident Management policy under ASU OP 44.00. Depending on the nature of the breach, other areas of the university may be involved, as designated by the program administrator.

4. Identification of Red Flags

After a comprehensive evaluation of the Angelo State University environment, the following items will be considered red flags:

a. Notifications and Warnings from Credit Reporting Agencies

(1) Report of fraud accompanying a credit report,

(2) Notice or report from a credit agency of a credit freeze on an applicant,

(3) Notice or report from a credit agency of an active duty alert for an applicant,

(4) Receipt of a notice of address discrepancy in response to a credit report request, and

(5) Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

b. Suspicious Documents

(1) Identification document or card that appears to be forged, altered or inauthentic;

(2) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

(3) Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and

(4) An application for service that appears to have been altered or forged.

c. Suspicious Personal Identifying Information

(1) Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates),

(2) Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report),

(3) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent,

(4) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address),

(5) Social security number presented that is the same as one given by another customer,

(6) An address or phone number presented that is the same as that of another person,

(7) 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), and

(8) A person's identifying information is not consistent with the information that is on file for the customer.

d. Suspicious Covered Account Activity or Unusual Use of Account

(1) Change of address for an account followed by a request to change the account holder's name,

(2) Payments stop on an otherwise consistently up-to-date account,

(3) Account used in a way that is not consistent with prior use (example: very high activity),

(4) Mail sent to the account holder is repeatedly returned as undeliverable,

(5) Notice to the university that a customer is not receiving mail sent by the university,

(6) Notice to the university that an account has an unauthorized activity,

(7) Breach in the university's computer system security, and

(8) Unauthorized access to or use of the customer's account information.

e. Alerts from Others

Notice to the university from a faculty, staff, or student, identity theft victim, law enforcement, or other person regarding possible identity theft in connection with covered accounts.

5. Detecting Red Flags

In order to detect the red flags for a new or existing account, university personnel will verify:

a. The identification of customers, if they request information (in person, via telephone, via facsimile, via email);

b. The validity of requests to change billing addresses; and

c. The accuracy of any banking information changes that impact billing and payment.

6. Consumer Credit Report Requests

In the event credit reports are required for an employment position, university personnel will take the following steps to detect red flags to identify address discrepancies:

a. Require written address verification from any applicant at the time the request for the credit report is made to the consumer reporting agency, and

b. Verify that the credit report pertains to the applicant for whom the requested report was made in the event of an address discrepancy. Personnel should notify the consumer-reporting agency and provide the relevant address information.

7. Response Actions

a. The program administrator will determine the appropriate response actions, if any, upon detection or report of red flags, in accordance with requirements of FACT Act and other applicable regulations. Such actions may include:

(1) Monitoring a covered account for evidence of identity theft;

(2) Contacting the customer;

(3) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(4) Reopening a covered account with a new account number;

(5) Not opening a new covered account;

(6) Closing an existing covered account;

(7) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(8) Notifying law enforcement; or

(9) Determining that no response is warranted under the particular circumstances.

b. The program administrator will log all reported red flag detections, along with the actions taken, to be included in the annual report for the vice president for finance and administration.

Appendix A

Angelo State University Areas That Must Comply With the Red Flag Rules

The following business areas and support units have been determined to fall under the requirements of the FTC Red Flag Rules and must appoint a representative to work with the Program Administrator:

- Student Accounts
- OneCard Office
- Human Resources
- Payroll Services
- Residence Life
- Financial Aid Office
- Information Technology
- Finance and Administration