[Date changed–posted 2/13/23 (last revised 6/15/21)]

TEXAS TECH UNIVERSITY

Operating Policy and Procedure

OP 62.14: Red Flag Rules

DATE: February 13, 2023

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 February of odd-numbered years by the Senior Managing Director of Cash and Credit Management Services with substantive revisions forwarded through administrative channels to the Associate Vice President for Financial & Business Services and the Senior Vice President for Administration & Finance and Chief Financial Officer.

POLICY/PROCEDURE

1. Definitions

a. Covered Accounts are those accounts identified in the Red Flag Regulations (see 16 CFR 681 *et seq.)* as a consumer account designed to permit multiple payments or transactions over time and any other account for which there is a reasonable foreseeable risk of identity theft. For purposes of this policy, it includes, but is not limited to, student financial accounts or other covered accounts maintained by TTU or its agents.

b. Creditor is 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 is a fraud committed or attempted by an individual using another person's identifying information to obtain money, items, or services, including education services, to which the individual is not entitled.

d. Identifying Information / Personally Identifiable Information (PII) is any name or number that may be used alone or with other information to identify an individual, including, but not limited to:

(1) Name, social security number, date of birth, telephone/cell number, government-issued driver's license or identification number, alien registration number, passport number, employer identification number (e.g., eraider), taxpayer identification number, protected health information (PHI), or credit/debit/banking account numbers;

(2) Unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation; or

(3) Unique electronic identification number, address, or routing code; IP or other computer identifying address; or telecommunication identifying information or other access device.

e. Red Flag is a pattern, practice, or specific activity involving an individual's identifying information that indicates the possible existence of identity theft to receive educational service from TTU.

2. General Policy

a. Texas Tech 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 Texas Tech 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 updated periodically to reflect environmental, institutional, and legal changes.

3. Program Oversight and Responsibility

a. The Senior Managing Director of Cash and Credit Management Services is designated as the program administrator, and he/she 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.

b. The program administrator is responsible for:

(1) Arranging for appropriate communication of the program details to departmental administration units that fall under Red Flag Rules;

(2) Providing basic training materials for department administrative employees to use to train employees (Red Flags Training);

(3) Providing a template to assist departments in complying with the program (Departmental Identity Theft Prevention Plan);

(4) Reviewing incident reports provided by departments; and

(5) Annually reviewing the program for potential changes.

c. Department administrative units managing or maintaining covered accounts are responsible for:

(1) Completing the Departmental Identity Theft Prevention Plan annually;

(2) Developing and implementing plans to effectively train their staff in the identification, detection, prevention, and mitigation of the Red Flags identified that are unique to their specific covered accounts; and

(3) Reviewing and updating their processes and procedures.

4. Identification of Red Flags

After a comprehensive evaluation of the Texas Tech 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; and

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

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 (e.g., a person's signature on a check appears forged); and

(4) 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 (e.g., inconsistent birth dates);

(2) Identifying information presented that is inconsistent with other sources of information (e.g., an address not matching an address on a credit report);

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

(4) Identifying information presented that is consistent with fraudulent activity (e.g., 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 (e.g., 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 unauthorized activity;

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

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

e. Alerts from Others

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

5. Detection of Red Flags

To detect the Red Flags identified above, the following actions will be taken, when appropriate given the particular covered account at issue and under the particular circumstances, to confirm the identity of students and individuals when they open and/or access their covered accounts:

a. Appropriate personal identifying information (e.g., photo identification, date of birth, academic status, username and password, address, etc.) shall be obtained from the student or individual account holder, prior to issuing a new or replacement ID card, opening a covered account, or allowing access to a covered account.

b. When certain changes to a covered account are made online, students and individuals holding covered accounts shall receive notification to confirm the change was valid and to provide instructions in the event the change is invalid.

c. Suspicious changes made to covered accounts that relate to an account holder's identity, administration of the account, and billing of the payment information shall be verified.

6. Prevention and Mitigation of Identity Theft

In addition to the efforts noted above to detect identity theft, university personnel involved in the administration of the covered accounts will take the following steps, where appropriate and based upon the particular circumstances, to prevent and mitigate occurrences of identity theft when a Red Flag is detected:

a. Monitor a covered account for evidence of identity theft;

b. Contact student(s) and/or individual account holder(s);

c. Request additional documentation from the student and/or individual account holder to verify identity;

d. Change passwords, security codes, and other security devices permitting access to the covered account;

e. Notify law enforcement;

f. Determine that no response is warranted under the particular circumstances;

g. Attempt to identify the cause and source of the Red Flag; or

h. Take appropriate steps to modify the applicable process to prevent similar activity in the future.