



TEXAS TECH UNIVERSITY™

Operating Policy and Procedure

OP 62.14: Red Flag Rules

DATE: May 28, 2010

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 June of odd-numbered years by the assistant vice president for financial affairs/controller with recommended revisions forwarded through administrative channels to the vice president for administration and 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., e-raider), 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 assistant vice president of financial affairs/controller 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.

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 Business Services
- Office of Student Financial Aid
- Graduate School
- Rawls College of Business - Center for Professional Development
- Edward E. Whitacre College of Engineering – Murdough Center for Engineering Professionalism/National Institute for Engineering Ethics
- Other covered accounts as identified will be notified by the program administrator.

- b. An annual program assessment shall be conducted and a report prepared including recommended program changes.
- c. The program administrator is responsible for:
 - (1) Developing, implementing, assessing, and updating the program;
 - (2) Developing and maintaining a training program;
 - (3) Ensuring compliance of university staff; and
 - (4) Reviewing any Red Flag detection reports and initiating the appropriate response actions.
- d. Any contract between TTU and a third party vendor who processes covered accounts for or on behalf of the university shall include language that the third party vendor agrees to comply with the Red Flag Regulations.

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;
 - (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 (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. Identity Theft and Protection

The program administrator shall periodically provide educational resources to designated individuals on the FTC Red Flag Rules and this policy.

Designated individuals are responsible to educate their staff on how to detect Red Flags that indicate possible identity theft. Schools, campuses, and departments with covered accounts shall

establish processes and procedures to detect Red Flags in connection with the opening of covered accounts and activity in existing covered accounts, such as the following:

a. Student Identity

(1) Student Business Services Office

Request information to verify the identity of a student or his/her parent or legal guardian requesting student financial information in person, or by telephone, facsimile, or e-mail. This information may include, but is not limited to, the presentation of photo ID (e.g., driver's license, passport, etc.), name, date of birth, home address, or other academic information on file with TTU. If the student or his/her parent or legal guardian is unable or unwilling to provide this information, notify the immediate supervisor in charge for further action.

(2) Office of Financial Aid

Student identity is verified through the Department of Education (DOE) from which TTU downloads information. Any discrepancies identified by the DOE are forwarded to the TTU Office of Financial Aid, which processes the notifications in accordance with federal and state laws.

b. Authentication of Students

At each in-person encounter, request photo identification to verify with the information in the file. If photo identification is not available, then request the individual provide an address, phone/cell number, last four digits of the social security number, or other unique identifying information. If the information is incorrect or suspicious, then notify the immediate supervisor for further action.

c. Requests for Changes

Verify the validity of requests to change the billing address, social security number, or other unique identifying information. Verification can include checking the proposed new information against an official document, such as a government issued ID for change of a social security number, or current utility bill for change of address.

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. In the event of an address discrepancy, verify that the credit report pertains to the applicant for whom the requested report was made. 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. For student covered accounts, the Records Custodian of

Education Records (FERPA Officer) shall promptly investigate instances of potential identity theft on student financial accounts and submit a confidential written report of findings to the program administrator. In accordance with requirements of the 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.
-