Texas Woman's University
University Regulation and Procedure

Regulation and Procedure Name:	**Red Flag Identity Theft**
Regulation and Procedure Number:	**URP: 04.200**
Policy Owner:	**Finance and Administration**

POLICY STATEMENT

The purpose of this policy is to establish an identity theft policy in accordance with the Federal Trade Commission Red Flag Rules which implement Section 114 of the Fair and Accurate Credit Transactions Act.

APPLICABILITY

This policy is applicable to TWU Employees.

DEFINITIONS

1. "Covered Accounts" means an account that the University offers or maintains that is designed to permit multiple payments or transactions. These include but are not limited to:

   a. Participation in Federal Perkins Loan Program

   b. Student emergency loan program

   c. Payment plans and promissory notes for covered student accounts

   d. Payment plans for covered employee accounts; i.e., parking permit, donations

   e. Use of the Pioneer Debit Card

2. "Identity Theft" means fraud committed or attempted using the identifying information of another person without authorization.

3. "Personally, Identifiable Information" means personally identifiable information is any information which may be used to uniquely identify, contact, or locate an individual. This 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PINs, personal account numbers, computer accounts and passwords, protected health information, financial information, unpublished home addresses or phone numbers, and any combination of information that will uniquely identify an individual.

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

REGULATION AND PROCEDURE

I. Authority and Responsibility

A. The Vice President for Finance and Administration is designated as the Program Administrator. The Program Administrator will work with departmental or unit administrators in areas affected by the Red Flag Rules. (*See* Attachment A for a list of these areas). The Program Administrator will also conduct an annual program assessment and provide a report to the Chancellor and President.

B. The Program Administrator is responsible for:

1. Developing, implementing, assessing and updating the Red Flag Program

2. Developing and maintaining a training program

3. Reviewing any red flag detection reports and initiating the appropriate response action

II. Detecting Red Flag Activity

A. New Covered Account

Possible red flags in connection with the establishment of a new Covered Account may include:

1. Address discrepancies

2. Presentation of suspicious documents

3. Photograph or physical description in the identification that is not consistent with the appearance of the person presenting the identification

4. Personal Identifying Information that is not consistent with other Personal Identifying Information that is on file with the University

5. Documents provided for identification that appear to have been altered or forged

B. Existing Covered Accounts

Possible red flags in connection with existing Covered Accounts may include:

1. Unusual or suspicious activity related to Covered Accounts

2. Notification from account holders, law enforcement, or service providers of unusual activity related to a Covered Account

3. Notification from a credit bureau of fraudulent activity regarding a Covered Account

4. A complaint or question from a Covered Account Holder based on the Covered Account Holder's receipt of:

   a. Bill for another individual

   b. Bill for a product or service the Covered Account Holder denies receiving

   c. Bill for a health care provider that the Covered Account Holder denies patronizing

5. A complaint or question from a Covered Account Holder about the receipt of a collection notice from a collection agency when the Account Holder believes there is no debt.

6. A dispute of a bill by a Covered Account Holder who claims to be the victim of any type of Identify theft

7. A statement from a Covered Account Holder that a bill was never received and the address on file is incorrect.

III. Methods to Prevent Identity Theft

Methods to prevent identity theft may include, but are not limited to the following actions:

A. Requiring each Covered Account Holder to provide photo identification at each "in person" encounter.

B. Requiring multi-factor identification before conducting any transaction over the phone with the Covered Account Holder relating to a Covered Account.

C. Requiring an on-line transaction to come through a secure, password protected portal or password protected e-mail account

D. Following up on each billing inquiry from a Covered Account Holder when the Covered Account Holder complains of suspicious activity

IV. Responding to Possible Red Flag Activity

Should an employee identify a Red Flag, the information must be brought to the attention of the supervisor, who in conjunction with the Program Administrator will investigate the threat to determine if there has been a breach. Additional actions may include notifying and cooperating with the Department of Public Safety or other law enforcement agencies.

V. Oversight of Service Providers

A. Texas Woman's University contracts with certain third party providers who receive information related to Covered Accounts or who handle Covered Accounts. Examples of third party providers contracted to provide services for Covered Accounts include:

1. Service provider to bill and collect Perkins Loans

2. Service provider to bill and collect Federal Nursing Loans

3. Student Account and emergency loan collection agencies

4. Service provider to distribute 1098T forms

5. Service provider to distribute student refunds

6. Service provider to maintain the payment gateway for student accounts

B. The Department Administrator responsible to oversee the service providers must require a written agreement with the third party providers that the third party provider has a program in place to ensure compliance with the Red Flag Rules.

VI. Periodic Update of Red Flag Program

The Red Flag Program will be reviewed annually by the Program Administrator. This review will include a risk assessment of potential identify theft possibilities.

REVIEW

This policy will remain in effect and published until it is reviewed, updated, or archived. This policy is to be reviewed once every six years. Interim review may be required as a result of updates to federal and state law or regulations, Board of Regents policies, or internal processes or procedures.

REFERENCES

None

FORMS AND TOOLS

None

Publication Date:	**07/02/2021**
Revised:	**07/02/2021**

Attachment A

Offices Identified as Conducting Services Covered Under the FTC Red Flag Rules:

- Financial Aid
- Bursar
- Department of Public Safety
- Student Health Services
- ID Card Services
- Student Life
- Payroll
- Institutional Development