SUL ROSS STATE UNIVERSITY

A Member of the Texas State University System

SRSU Policy: Identity Theft Prevention Program ("Red Flags Rule")
SRSU Policy ID: APM 3.13
Policy Reviewed by: Vice President for Finance and Operations
Approval Authority: Executive Council
Approval Date: 07/15/25
Next Review Date: 07/15/30

POLICY

Sul Ross State University is committed to properly managing covered accounts to safeguard against
identity theft. In compliance with the Federal Trade Commission's (FTC) Red Flags Rule and the Texas State University System's (TSUS) Rules and Regulations, Sul Ross State University has developed an Identity Theft Prevention Program that includes reasonable policies and procedures to detect, identify, mitigate, and prevent identity theft in connection with covered accounts.

PURPOSE AND SCOPE

This policy sets forth the Sul Ross State University Identity Theft Prevention Program ("Program"), which has been developed to comply with the TSUS Rules and Regulations, Section III, 6(20) and with
the Red Flags Rule (16 C.F.R. 681) issued by the Federal Trade Commission (FTC) and pursuant to
the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Sul Ross State University has established a Program that is appropriate to the size and complexity of its financial systems and operations and the nature and scope of its activities.

Sul Ross State University's Program shall minimally address the following areas, to the extent applicable to the University's operations:

1. Issuance of student identification cards;
2. Use of background checks;
3. Handling of consumer accounts that involve multiple payments, including but not necessarily limited to the following:
    a. The federal Perkins Loan Program;
    b. The federal Family Education Loan Program;
    c. Institutional loan programs for students, faculty, or staff; or,
    d. Institutional tuition (or fee) installment payment plans (Texas Education Code § 54.007).

DEFINITIONS

Covered Accounts. An account designated to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk of identity theft.

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

Personal Identifying Information. Any name or number that may be used, alone or in conjunction
with any other information, to identify a specific person, including but not limited to:

- name;
- address;
- telephone number;
- Social Security number;
- date of birth;
- government issued driver's license or identification number;
- alien registration number;
- government passport number;
- employer or taxpayer identification number;
- student identification number;
- computer Internet Protocol address; or
- routing code.

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

ROLES AND RESPONSIBILITIES

The **Sul Ross State University Executive Council** shall approve any updates to the Program and this policy.

Program Administrator. As authorized by TSUS, the Sul Ross State University President has designated the Vice President for Finance and Operations as the Program Administrator.

1. The Program Administrator is the primary administrator empowered to manage and execute all aspects of the Program, including the engagement of other institutional departments and personnel as necessary to detect, identify, mitigate, and prevent identity theft.
2. The Program Administrator shall:
    a. provide oversight of the Program (including training and appropriate actions);
    b. periodically review the Program and make updates to account for environmental, institutional, technological, and legal changes;
    c. annually report to the President on incidents involving identity theft, management's response, and recommended Program changes;
    d. develop procedures for execution of the Program; and
    e. manage outside service providers.

Third-party Service Providers. In the event Sul Ross State University engages a third-party service
provider to perform an activity in connection with one or more covered accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures to detect, identify, mitigate, and prevent the risk of identity theft:

1. Require that the service provider provide written documentation certifying their compliance with the Red Flags Rule to the offices that contracted their services.
2. Require that the service provider report any Red Flags to the Program Administrator or to the University employee with primary oversight of the service provider relationship (this employee will then report any Red Flags to the Program Administrator).

EMPLOYEE TRAINING
Sul Ross State University is working towards employee awareness of Red Flags Rule through the Offices of Finance and Human Resources with training.

IDENTIFYING RED FLAGS
To identify relevant Red Flags, Sul Ross State University considers the types of accounts that it offers and maintains, the methods it provides to open and access covered accounts, and its previous
experiences with identity theft.

The following items are considered Red Flags (risk factors):

1. Notifications and warnings from credit reporting agencies;
2. The presentation of suspicious documents, such as inconsistent photo identification or personal identifying information;
3. The presentation of suspicious personal identifying information, including personal information inconsistent with other information on file;
4. Suspicious covered account activity or unusual use of account; and
5. Alerts from persons or entities outside the University.

DETECTING RED FLAGS
Sul Ross State University personnel will verify:

1. The identification of individuals requesting information about themselves or their accounts
2. whether the request is made in person or via telephone, facsimile, email, or other means.
3. The validity of a request to change account-related addresses or contact information.
4. The accuracy of changes in bank account information that might impact billing and payment.

RESPONDING TO RED FLAGS
Sul Ross State University personnel will notify the Program Administrator upon identifying a Red Flag. The Program Administrator will determine appropriate response actions. Such actions will be made to mitigate identity theft and may include, but are not limited to, the following:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the affected individual;
3. Changing any passwords, security codes, or other security measures that permit access to a covered account;
4. Notifying law enforcement; or
5. Determining that no response is warranted under the particular circumstances.

The Program Administrator shall notify the Information Security Officer (ISO) if the Red Flag suggests the possibility of a breach in information security.

The Program Administrator will log all reported Red Flag detections and actions taken. This information will be included in the Program Administrator's annual report to the President.