

Sam Houston State University
A Member of The Texas State University System

Finance & Operations Policy FO-57
Identity Theft Prevention Program

Purpose: This document institutes the Sam Houston State University Identity Theft Prevention Program (“Program”) in compliance with the *Red Flags Rule* (16 C.F.R. 681), issued by the Federal Trade Commission and pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA). The Program establishes reasonable policies and procedures, appropriate to the size and complexity of the University’s activities, to detect, prevent, and mitigate identity theft in connection with a covered account.

Program Requirements: As authorized by the Texas State University System, the Sam Houston State University President had designated the Vice President for Finance & Operations as the Program Administrator. The Program Administrator will:

- Develop and implement a written Identity Theft Prevention Program;
- Provide oversight of that Program (including training and appropriate actions);
- Periodically review the Program with the President and update the Program to reflect changes in identity theft risks and technology; and
- Regularly report to the President on the effectiveness of the Program, including an annual written report.

The President’s Approval shall be sufficient to make changes to the Program.

POLICY/PROCEDURE

1. Definitions

- a. Covered Accounts. A consumer account designated to permit multiple payments or transactions, or any other account for which there is a reasonable foreseeable risk for the identity theft.
- b. Identity Theft. Fraud committed or attempted using the identifying information of another person without authorization.
- c. Personal Identifying Information. Is 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’s Internet Protocol address, or routing code.
- d. Program Administrator: The individual designated with primary responsibility for oversight of the Identity Theft Prevention program mandated by the FTC’s *Red Flags Rule*.
- e. Red Flag. A pattern, practice, or specific activity that indicates the possible existence of identity theft.

2. General Policy

- a. Sam Houston State University is committed to protecting all personal identifying information and preventing identity theft, as required by the *Red Flags Rule*.
- b. As required by the *Red Flags Rule*, the Program includes the following policy specifics:
 - i. identifying relevant Red Flags for new and existing covered accounts;
 - ii. detecting Red Flags that have been incorporated into the Program; and

Sam Houston State University
A Member of The Texas State University System

- iii. 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, technological, and legal changes.

3. Authority and Responsibility

- a. The Vice President for Finance and Operations is the University's designated Program Administrator and will exercise appropriate and effective Program oversight. The Program Administrator shall be 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.
- b. Periodically, the Program Administrator shall discuss assessments of the Program with the University President. The Program Administrator shall provide an annual report to the President, to include incidents involving identity theft, management's response, and recommended Program changes.
- c. The Program Administrator is responsible for ensuring the completion of the following seven steps for compliance:
 - i. analyzing the size and complexity of the University covered accounts;
 - ii. determining the existing policies that control foreseeable risks of identity theft;
 - iii. developing a list of "Red Flags" (risk factors) for the covered accounts and how to detect them;
 - iv. establishing the procedures that should be followed when a Red Flag is detected;
 - v. training the University employees who work with covered accounts;
 - vi. evaluating the program administration and regularly updating the Program to reflect changes in risk;
 - vii. managing outside service providers.
- d. Third party vendors who process payments for or on behalf of the University must provide written documentation certifying their compliance with the FTC's *Red Flags Rule*.
- e. To assure the Program's effectiveness, specific details of the Program's identification, detection, mitigation, and prevention practices are considered "confidential" information and shared with employees according to their "need to know".
- 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.

4. Identification of Red Flags

To identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open/access its covered accounts, and its previous experiences with identity theft. The following items will be considered Red Flags (risk factors):

- a. Notifications and Warnings from Credit Reporting Agencies
- b. The Presentation of Suspicious Documents, such as inconsistent photo identification or personal identifying information

Sam Houston State University
A Member of The Texas State University System

- c. The Presentation of Suspicious Personal Identifying Information –Personal information inconsistent with other information on file
- d. Suspicious Covered Account Activity or Unusual Use of Account
- e. Alerts from Others

5. Employee Training

Each employee who works with a covered account shall attend annual training on the Program. The Controller's Office will offer Program training in conjunction with IT Security. The training will include review of the relevant policies and procedures on how to manage covered accounts, guidance on how to detect Red Flags, as well as procedures for responding to Red Flags.

6. Detecting Red Flags

University personnel will verify:

- a. the identification of customers requesting information about themselves (in person, via telephone, via facsimile, via email);
- b. the validity of request to change account-related addresses; and
- c. the accuracy of changes in bank account information that might impact billing and payment.

7. Response Actions

- a. Notification of a Red Flag will be made to the Program Administrator immediately after its identification. The Program Administrator will determine the appropriate response of actions, if any, upon detection or report of Red Flags, in accordance with requirements of the FACT Act of 2003 and other applicable regulations. The Program Administrator shall notify IT Security if the Red Flag suggests the possibility of a breach in information security. Such actions will be made to mitigate identify theft, and may include but are not limited to:
 - i. monitoring a covered account for evidence of identity theft.
 - ii. contacting the customer;
 - iii. changing any passwords, security codes, or other security devices that permit access to a covered account;
 - iv. notifying the law enforcement; or
 - v. 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 and include a summary in the annual report for the President.

8. Continually Administer and Regularly Update

- a. The Program will be periodically reviewed and updated to reflect changes in identity theft risks, business practices and procedures, and the technological environment. In reflecting upon possible changes, the Program Administrator will consider:
 - i. The University's experiences with identity theft;

Sam Houston State University
A Member of The Texas State University System

- ii. changes in identity theft methods;
 - iii. changes in types of accounts the University maintains;
 - iv. changes in the University's business arrangements with other entities; and
 - v. any changes in legal requirements in the area of identity theft.
- b. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted.

9. Outside Service Provider Arrangements

- a. In the event the University engages a service provider to perform an activity in connection with one or more accounts, the service provider is required to provide written documentation certifying their compliance with the *FTC Red Flags Rule*.

Date Approved: President's Cabinet- 4/05/2010

Reviewed by: Dana L. Gibson - Vice President for Finance & Operations- 4/5/2010

Next review: 3/15/2011