**University Identity Theft UPPS No. 05.04.10**

**Prevention Program Issue No. 1**

**Effective Date: 05/29/2018**

**Next Review Date: 02/01/2023 E5Y**

**Senior Reviewer: Treasurer**

1. **POLICY STATEMENTS**
	1. This policy sets forth the Texas State University Identity Theft Prevention Program in compliance with the [*Red Flags Rule* (16 C.F.R. 681),](https://www.ftc.gov/policy/federal-register-notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and) issued by the Federal Trade Commission (FTC) and pursuant to the [Fair and Accurate Credit Transactions Act of 2003 (FACTA)](https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003). The program establishes reasonable policies and procedures to detect, prevent, and mitigate identity theft in connection with a covered account.
	2. President’s Cabinet members endorsed the program with the understanding that specific details of the program are considered confidential information and shared with employees according to their need to know.
	3. Treasurer’s Office and Information Security staff will continue to monitor activities, identifying areas where supplemental policies need to be developed.
2. **DEFINITIONS**
	1. Covered Accounts – a consumer account designated to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk for identity theft.
	2. Identity Theft – fraud committed or attempted using the personal identifying information of another person without authorization.
	3. 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’s internet protocol address, or routing code.
	4. Program Administrator – the individual designated with primary responsibility for oversight of the Identity Theft Prevention Program mandated by the FTC’s [*Red Flags Rule*](https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf). As authorized by The Texas State University System, the president has designated the vice president for Finance and Support Services as the program administrator.
	5. Red Flag – a pattern, practice, or specific activity that indicates the possible existence of identity theft.
3. **GENERAL POLICY**
	1. Texas State is committed to protecting all personal identifying information and preventing identity theft, as required by the [*Red Flags Rule*](https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf).
	2. As required by the [*Red Flags Rule*](https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf), the program includes the following policy specifics:
4. identifying relevant red flags for new and existing covered accounts;
5. detecting red flags that have been incorporated into the program; and
6. responding appropriately to detected red flags in order to prevent and mitigate identity theft.
	1. The program will be reviewed periodically to reflect environmental, institutional, technological, and legal changes. The president’s approval shall be sufficient to update or make changes to the program.
	2. The Treasurer’s Office will coordinate with all the identified stakeholder departments to complete and remit to the program administrator, on a quarterly basis, a Red Flag Incident Reporting Log. The log will identify all stakeholders, and if an incident was reported, identify dates, departments, issue and response, and if the issue was resolved or is still pending.
7. **AUTHORITY AND RESPONSIBILITY**
	1. The vice president for Finance and Support Services 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.
	2. Periodically, the program administrator shall discuss assessments of the program with the 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 if appropriate.
	3. The program administrator is responsible for ensuring the completion of the following seven steps for compliance:
8. analyzing the size and complexity of the university covered accounts;
9. determining the existing policies that control foreseeable risks of identity theft;
10. developing a list of red flags (risk factors) for the covered accounts and how to detect them;
11. establishing the procedures that should be followed when a red flag is detected;
12. training university employees who work with covered accounts;
13. evaluating the program administration and discussing with the president recommendations to regularly update the program to reflect changes in risk; and
14. managing outside service providers.
	1. 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*](https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf)to the offices which contracted their services.
	2. 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.

04.06 In the event university personnel detect any identified red flags or related suspicious activity, such personnel shall research the issue and if the issue is not instantly remedied, report it immediately to the program administrator. The program administrator will conduct further investigation and initiate the appropriate response actions. If the issue is remedied, it will be reported on a quarterly report issued to the program administrator.

1. **IDENTIFICATION OF RED FLAGS**
	1. To identify relevant red flags, the university considers the types of accounts that it offers and maintains, the methods it provides to open and access its covered accounts, and its previous experiences with identity theft. The following items will be considered red flags (risk factors):
2. notifications and warnings from credit reporting agencies;
3. the presentation of suspicious documents, such as inconsistent photo identification or personal identifying information;
4. the presentation of suspicious personal identifying information, including personal information inconsistent with other information on file;
5. suspicious covered account activity or unusual use of account; and
6. alerts from persons or entities outside of the university.
7. **EMPLOYEE TRAINING PROCEDURES**
	1. Each employee who works with a covered account shall attend training as necessary. Staff who have taken fraud prevention training may not need to be re-trained on the program.
	2. All new staff who work with a covered account must take the training within sixty business days of their position start date.
	3. The Treasurer’s Office will offer program training in conjunction with the Information Security Office (ISO). 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.
8. **PROCEDURES FOR DETECTING RED FLAGS**
	1. To detect red flags, university personnel will verify:
9. the identification of customers requesting information about themselves (in person, via telephone, via facsimile, via email);
10. the validity of requests to change account-related addresses; and
11. the accuracy of changes in bank account information that might impact billing and payment.
12. **RESPONSE ACTIONS**
	1. Notification of a red flag will be made to the program administrator immediately after its identification, if not instantly remedied. The program administrator will determine the appropriate response actions, if any, upon detection or report of red flags, in accordance with requirements of the [FACT Act of 2003](https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003) and other applicable regulations. If the issue is remedied, the instance will be reported on the quarterly report submitted to the program administrator.

* 1. The program administrator shall notify the ISO if the red flag suggests the possibility of a breach in information security. Such actions will be made to mitigate identity theft, and may include but are not limited to:
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. notifying law enforcement; or
5. determining that no response is warranted under the particular circumstances.
	1. The program administrator will supply a summarized log of all reported red flag detections along with the actions taken and if the issue has been resolved in an annual report for the president.
6. **PROCEDURES FOR REGULAR PROGRAM REVIEW**
	1. The program will be periodically reviewed to reflect changes in identity theft risks, business practices and procedures, and the technological environment,
	2. In reflecting upon possible changes, the program administrator will consider:
7. the university’s experiences with identity theft;
8. changes in identity theft methods;
9. changes in types of accounts the university maintains;
10. changes in the university’s business arrangements with other entities; and
11. any changes in legal requirements in the area of identity theft.
	1. After considering these factors, the program administrator will determine whether changes to the program, including the listing of red flags, are warranted.
12. **OUTSIDE SERVICE PROVIDER ARRANGEMENTS**
	1. 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*](https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf)to the offices which contracted their services.
13. **REVIEWERS OF THIS UPPS**
	1. Reviewers of this UPPS include the following:

Position Date

Treasurer February 1 E5Y

Director, Student Business Services February 1 E5Y

Chief Information Security Officer February 1 E5Y

1. **CERTIFICATION STATEMENT**

This UPPS has been approved by the following individuals in their official capacities and represents Texas State policy and procedure from the date of this document until superseded.

Treasurer; senior reviewer of this UPPS

Vice President for Finance and Support Services

President