

1. Title

Identity Theft Prevention, Detection, and Mitigation Program

2. Policy

Sec. 1 Purpose. The purpose of this Policy is to provide for the development and implementation of a written Identity Theft Prevention, Detection, and Mitigation Program (Program) at U. T. System Administration to help identify, detect, and respond to patterns, practices, or specific activities, known as “Red Flags,” that could indicate identity theft.

Sec. 2 Policy Statement. It is the Policy of The University of Texas System Administration to take all reasonable steps and to implement all reasonable procedures to detect, prevent, and mitigate identity theft, pursuant to federal rules and regulations. In particular, it is the policy of U. T. System Administration to take all reasonable steps and to implement all reasonable procedures to detect, prevent, and mitigate identity theft, with respect to “covered accounts,” as defined in this Policy, and to meet the requirements of the Red Flag Rules established by the Federal Trade Commission and other federal agencies.

Sec. 3 Red Flag Rules Requirement. The Federal Trade Commission Red Flag Rules (Rules) require the development and implementation of a written Identity Theft Prevention, Detection, and Mitigation Program for affected businesses and governmental agencies, including universities that defer payment for goods or services. The Rules provide flexibility to design a Program appropriate for the particular size and the potential risks of identity theft unique to U. T. System Administration.

Sec. 4 Procedures.

4.1 The System-wide Chief Information Security Officer will establish a list of all departments and offices identified as holding covered accounts that are subject to the Program, and will be responsible for oversight, compliance, and periodic risk assessment to keep the Program up to date and to keep the department or office in compliance with the Program and the Red Flag Rules. [See [Appendix A.](#)]

4.2 The System-wide Chief Information Security Officer will set a schedule for identification of the relevant Red Flags associated with the covered accounts within each department and office. [See [Appendix A.](#)]

- 4.3 The System-wide Chief Information Security Officer will establish practices and procedures designed to
- (a) detect the presence of Red Flags in connection with all covered accounts that the program incorporates,
 - (b) respond appropriately to detected Red Flags to determine if identity theft is occurring or may occur,
 - (c) prevent the occurrence or terminate the ongoing identity theft if possible, and
 - (d) mitigate any identity theft that has occurred.

[See Appendices [A](#), [B](#), and [C](#).]

- 4.4 All U. T. System Administration departments and offices periodically, but no less than annually, must conduct a risk assessment to determine if they have become responsible for covered accounts that require the department or office to be added to the Program. [See [Appendix C](#).]

- 4.5 The System-wide Chief Information Security Officer will review the Program and update periodically, but no less than annually, to reflect changes in risk associated with identity theft by performing an assessment of the experiences of each department or office, since the previous review, with respect to
- (a) number and type of incidents of identity theft occurring since the last review;
 - (b) changes in methods of identity theft;
 - (c) changes in the type of accounts that the department or office maintains; and
 - (d) changes in methods to detect, prevent, and mitigate identity theft.

[See [Appendix C](#).]

- 4.6 The System-wide Chief Information Security Officer will provide initial training and periodic additional training of all U. T. System Administration staff as necessary to implement and enforce the Program effectively. [See [Appendix C](#).]

- 4.7 The System-wide Chief Information Security Officer will report annually to the Chancellor to ensure compliance with the Program. The report shall address material matters related to the Program and evaluate issues such as
- (a) the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts,
 - (b) third party service provider agreements relating to covered accounts,
 - (c) significant incidents involving identity theft and management's response, and
 - (d) recommendations for material changes to the Program.

[See [Appendix C.](#)]

3. Definitions

Account - any continuing relationship between U. T. System Administration and an Account Holder that permits the Account Holder to obtain a product or service for personal, family, household, or business purposes. It may involve the extension of credit for the purchase of a product or service, or a deposit account.

Account Holder - A student, employee, retired employee, patient, or other person that has a covered account held by or on behalf of U. T. System Administration.

Covered Account - an account U. T. System Administration offers or maintains or an account that is offered or maintained by a vendor or other third party on behalf of U. T. System Administration, primarily for personal, family, or household purposes, and that involves or is designed to permit multiple payments or transactions; and any other account U. T. System Administration offers or maintains for which there is a reasonably foreseeable risk to an Account Holder or to the safety and soundness of U. T. System Administration from identity theft, including financial, operational, compliance, reputation, or litigation risks. Examples of covered accounts include, but are not limited to student loan and tuition accounts, patient medical service accounts, accounts associated with employee benefits, student debit cards, and meal plans.

Identity Theft - any use or attempt by an individual to use another person's individual identifying information to obtain a thing of value including money, credit, items, or services, such as medical care or education services, to which the individual is not entitled.

Individual Identifying Information - any information 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 or taxpayer identification number, 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, Internet Protocol (IP) or other computer identifying address, or telecommunication identifying information or other access device.

Red Flag - suspicious patterns or practices, or specific activities that indicate the possibility that identity theft may occur or is occurring in connection with U. T. System Administration's covered accounts.

Responsible Party - appropriate senior officer or employee with sufficient training, experience, and authority to develop, maintain, and oversee compliance with U. T. System Administration's Program.

4. Relevant Federal and State Statutes, Policies, and Standards

[Fair and Accurate Credit Transactions Act of 2003 \(FACTA\), 16 CFR 681.2, the Federal Trade Commission's \(FTC\) Red Flag Rules](#)

[FTC summary of the steps required to comply with the Red Flag Rules](#)

[FTC "How to Guide for Businesses" 17 pages](#)

5. Relevant System Policies, Procedures, and Forms

[Appendix A: Possible Red Flags in Connection with a Covered Account](#)

[Appendix B: Prevention and Mitigation; Oversight of Third Party Service Providers](#)

[Appendix C: The University of Texas System Administration Identity Theft Prevention, Detection and Mitigation Program](#)

[Sub-Program #1: Accounting and Purchasing Services within Operations and Support Services](#)

[Sub-Program #2: Claims and Financial Litigation Section within the Office of General Counsel](#)

[Sub-Program #3: Office of Employee Benefits](#)

[UT System Information Security Incident Reporting Toolkit](#)

6. System Administration Office(s) Responsible for Policy

Office of System-wide Information Services

7. Dates Approved or Amended

July 1, 2009

October 30, 2009

November 19, 2012