UTDBP3037

Policy on Identity Theft Prevention Detection and Mitigation Program

Policy Statement

Policy Overview

The University of Texas at Dallas (the University) has developed an Identity Theft Prevention, Detection and Mitigation Program to detect, prevent and mitigate Identity Theft pursuant to the Federal Trade Commission Red Flags Rule 16 CFR 681.1 in accordance with FTC enforcement of the Fair and Accurate Transactions Act of 2003 15 U.S.C 1681s(a)(1). The program is effective August 1, 2009, and will be maintained and updated annually.

Definitions

Account: An Account is any continuing relationship between the University 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 the University.

Covered Account: An Account the University offers or maintains or is offered or maintained by a vendor or other third party on behalf of the University primarily for personal, family, or household purposes. The Account involves or is designed to permit multiple payments or transactions; to include any other Account the University offers or maintains for which there is a reasonably foreseeable risk to an Account Holder or to the safety and soundness of the University from Identity Theft, including financial, operational, compliance, reputation, or

litigation risks. Examples of Covered Accounts include, but are not limited to student loans 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 to which the individual is not entitled including: money, credit, items, or services, such as medical care or education services.

Individual Identifying Information: Any information that may be used alone or with other information to identify an individual, including, but not limited to: (1) personal identifiable information such as 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 information such as identification number, address or routing code, IP or other computer identifying address, or telecommunication identifying information or other access device.

Red Flag: Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility that Identity Theft may occur or is occurring in connection with the University's Covered Accounts.

Reasonable Parties

The University President has appointed the Vice President for the Office of Budget and Finance to be the Executive Sponsor of the Program. The Executive Sponsor has appointed the Chief Information Security Officer as the Program Administrator. The Program Administrator's responsibility is to develop and maintain a comprehensive university wide program, which includes:

- Completing a university wide risk assessment to identify departments which have Covered Accounts,
- Maintaining a list of offices and departments identified as holding covered accounts subject to the Program.
- Ensuring the appointment of Departmental Program Coordinators for departments that have Covered Accounts,
- Providing leadership and guidance to the Departmental Program Coordinators in the initial development and the on-going maintenance of the program,
- Developing training material and coordinating the training program, Coordinating risk

assessment and compliance reporting
- Performing initial and annual risk assessments in the departments identified having Covered Accounts,
- Developing the program for their Covered Accounts and ensuring that the program elements are commensurate with the level of risk identified,
- Ensuring that staff in their departments have been trained on the elements as it pertains to their respective job responsibilities and that the training is effective, and
- Preparing reports on the status of the program.

Elements of UTD's Identity Theft Program

The University has developed and implemented an Identity Theft Prevention, Detection and Mitigation Program. The program includes:

- A list of Covered Accounts that are subject to the program, and the officer or employee responsible for oversight, compliance and periodic risk assessment to keep the program up to date and to keep the department in compliance with the program.
- Identification of the relevant "Red Flags" associated with the Covered Accounts within each department and office.
- Practices and procedures designed to:
    1. Detect the presence of Red Flags in connection with all Covered Accounts that the program incorporates,
    2. Respond appropriately to detected Red Flags to determine if Identity Theft is occurring or may occur,
    3. Prevent the occurrence or terminate the ongoing Identity Theft if possible, and
    4. Mitigate any Identity Theft that has occurred.
- A requirement that the Program Administrator and the Departmental Program Coordinators periodically, but not less than annually, conduct a risk assessment to determine if changes to the existing program are required. In reviewing the program, the following factors should be considered:
    1. Incidents of Identity Theft occurring since the last review,
    2. Changes in methods of Identity Theft,
    3. Changes in the type of Cover Accounts that the department maintains, and
    4. Changes in methods to detect, prevent, and mitigate Identity Theft.
- A requirement that the University provide initial training and periodic additional training to staff as necessary to implement and enforce the program effectively.
- A requirement for compliance reports to ensure compliance with the program.

Oversight of Third Party Service Providers

The University will require a written agreement that third party service providers who receive information related to the University's Covered Accounts or who otherwise handle the University's Covered Accounts, have a documented program in place that ensures compliance by the third parties with the Red Flags Rule with respect to the University Covered Accounts; or adopt and comply with the University's program.

Reporting

The Program Administrator will prepare an annual report, which will include the following:

1. The effectiveness of the policies and procedures in addressing the risk of Identity Theft,
2. Status of third party service provider agreements relating to Covered Accounts,
3. Significant incidents involving Identity Theft and management's response, and
4. Recommendations for material changes to the program.

RESPONSIBLE PARTY

LAST REVIEWED

-

HISTORY

- Issued: 2009-08-01
- Revised: 2018-05-11