Identity Theft Prevention, Detection and Mitigation

Responsible Officer: Vice President for Business Affairs and Controller
Sponsoring Department: Accounting Services
Revision Date: 01 May 2009
Errors or changes to: aim@uta.edu

Contents

I. Overview
II. Definitions
III. Contacts
IV. Procedures

I. Overview

The University of Texas at Arlington will develop, maintain and update an Identity Theft Prevention, Detection and Mitigation Program ("Program") to detect, prevent and mitigate identity theft in accordance with the 16 CFR 681.2, the Federal Trade Commission’s "Red Flag Rules."

II. Definitions

A. Account: 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.

B. Account Holder: Student, Employee, Retired Employee, Patient or other person that has a Covered Account held by or on behalf of the University.

C. 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, that involves or is designed to permit multiple payments or transactions; and 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 loan and tuition accounts; patient medical service Accounts; Accounts associated with employee benefits; student debit cards; and meal plans.

D. 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.

E. **Individual Identifying Information**: Individual Identifying Information is 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; IP or other computer identifying address; or telecommunication identifying information or other access device.

F. **Red Flag**: 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.

G. **Responsible Party**: Appropriate senior officer or employee with sufficient training, experience and authority to develop, maintain, and oversee compliance with the University’s Program.

III. **Contacts**

The Office of Business Affairs is responsible for this policy.

IV. **Procedures**

A. **RESPONSIBLE PARTY**

The President has appointed the Vice President for Business Affairs and Controller to be the Responsible Party for the University of Texas at Arlington’s Identity Theft Prevention, Detection and Mitigation Program.

The Vice President for Business Affairs and Controller will develop a written Identity Theft Program that requires each department or office within the University to conduct a risk assessment to determine what university accounts, within the responsibility of the department or office, are considered covered accounts. The risk assessment must take into consideration the method the university provides to open its accounts; the method the University provides to access its accounts; and the University’s previous experiences with identity theft. The Vice President for Business Affairs and Controller, as appropriate, may incorporate into the Program any existing policies and procedures that promote the purpose of the Program. The Vice President for Business Affairs and Controller may also incorporate information security tools currently available at the University, to the extent these tools can assist with implementation of the Program.

The President must approve the initial Identity Theft Program.
B. ELEMENTS OF AN IDENTITY THEFT PROGRAM

The Program must include:

A list of all departments and offices identified as holding 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 or office in compliance with the Program and the Red Flag Rules.

Practices and procedures designed to:

- Identify Red Flags for covered accounts and incorporate them into the program
- Detect the presence of Red Flags in connection with all covered accounts that the program incorporates;
- Respond appropriately to detected Red Flags to prevent and mitigate identity theft
- Update the program periodically to reflect changes in risks

A requirement that all university departments and offices periodically, but no less than annually, 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.

A requirement that the Program be reviewed and updated 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:

- incidents of Identity Theft occurring since the last review;
- changes in methods of identity theft;
- changes in the type of accounts that the department or office maintains; and
- changes in methods to detect, prevent and mitigate identity theft.

A requirement that the University must provide initial training and periodic additional training of all University staff as necessary to implement and enforce the Program effectively.

A requirement that the Vice President for Business Affairs and Controller make periodic reports to an appropriate officer or committee to ensure compliance with the Program.

To the extent the University utilizes a third party who receives information related to University's covered accounts or who otherwise handles University's
Covered Accounts, the University will require via written agreement that the third party:

- have a written Program in place that ensures compliance of the third party with the Red Flag Rules with respect to all University Covered Accounts; or

- adopt and comply with the University’s Program with respect to all University Covered Accounts.

C. REPORTING

The Vice President for Business Affairs and Controller shall report to the President, at least annually on compliance with the Program.

The report shall address material matters related to the Program and evaluate issues such as:

- 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;

- third Party service provider agreements relating to Covered Accounts;

- significant incidents involving identity theft and management’s response; and

- recommendations for material changes to the Program.

D. IDENTIFY RELEVANT RED FLAGS

Five categories of "Red Flags" are:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers

- Presentation of suspicious personal identifying information

- Presentation of suspicious documents

- Unusual use of, or other suspicious activity related to, a covered account

- Notice from Account Holder, victims of identity theft, or law enforcement authorities

Possible methods of detection of "Red Flags" include:

- Any unusual or suspicious activity related to Covered Accounts

- Notification from account holders, law enforcement, or service providers of unusual activity related to a Covered Account
• Notification from a credit bureau of fraudulent activity regarding a Covered Account

• Photograph or physical description on the identification that is not consistent with the appearance of the person presenting the identification

• Individual Identifying Information provided by a person to establish a Covered Account that is not consistent with other personal identifying information on file with the University

• A complaint or question from an Account Holder based on the Account Holder's receipt of:
  • a bill for another individual
  • a bill for a product or service that the Account Holder denies receiving
  • a bill from a health care provider that the Account Holder denies patronizing; or
  • a notice of health plan benefits or other third party payor payments made on behalf of an Account Holder (such as an Explanation of Benefits) for health services the Account Holder never received.

• Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the Account Holder.

• A complaint or question from an Account Holder about the receipt of a collection notice from a bill collector.

• An Account Holder or third party payor report that coverage for legitimate hospital stays is denied because benefits have been depleted or a lifetime cap has been reached.

• A complaint or question from an Account Holder about information added to a credit report by a health care provider or third party payor.

• A dispute of a bill by an Account Holder who claims to be the victim of any type of Identity Theft.

• An Account Holder who claims to have a health plan or other third party coverage or eligibility but never produces an identity card or other physical documentation of the coverage or eligibility.

• A notice or inquiry from an insurance fraud investigator for a private insurance company or a state or federal regulatory or law enforcement agency.
A statement from an account holder that a bill or Explanation of Benefits was never received and the address on file is incorrect.

Mail sent to the account holder is returned repeatedly as undeliverable, although charges continue to accrue on the covered account.

Requiring each Account Holder to provide photo identification at each "in person" encounter, and in the case of an Account Holder seeking medical services or products, requiring a copy of the third party payor identification card at each encounter. Note: This detection method may not be appropriate for minors, indigent patients with no insurance, and emergency cases. Each department or office should determine in the risk assessment if requesting identification is unduly burdensome on their account holder population in light of the risk of Identity Theft in that population.

Requiring multi-factor identification before conducting any transaction relating to a Covered Account with an Account Holder over the telephone.

Requiring that on-line transactions come through a secure, password protected portal or in the case of a University employee, a verifiable, secure password protected University e-mail account.

Thoroughly following up on each billing inquiry from Account Holders, especially inquiries regarding care that was not received, bills for individuals not covered by the Covered Account or policies held, or bills from other health care providers that the Account Holder never visited.

Periodically auditing medical records to ensure that treatment is consistent for a single individual.

E. PREVENTION AND MITIGATION

Appropriate responses to prevent or mitigate identified possible or actual Identity Theft may include:

- Placing an alert on the record to make all applicable University employees aware that there may be a problem. In some cases, an alert may be requested by the Account Holder.

- Monitor accounts

- Change any passwords or other authenticating codes related to the Covered Account

- Notification of the Account Holder of the possible or actual Identity Theft in situations where notification is necessary to or likely to permit the Account Holder to take action to protect him or herself from the consequences of the Identity Theft.

- Correcting erroneous demographic information in the Covered Account record.
File extraction-purging the Account Holder’s file to the extent possible of all information that was entered as a result of the fraudulent activity, and replacing with a brief cross-reference and explanation of the deletion. The purged information is then placed into a new file.

- Notify law enforcement

- Closing the Covered Account for the Account Holder and opening a new one with a new account number.

- Determining that no response is warranted under the particular circumstances.