



UT System Administration Policy Library -- Policy

INT 162 - Identity Theft Prevention, Detection and Mitigation Program

Responsible Officer: Vice Chancellor for Administration

Sponsoring Office: Office of Administration

Effective Date: July 1, 2009

Last Reviewed: October 30, 2009

Errors or changes to: policyoffice@utsystem.edu

CONTENTS

Policy Statement

Rationale

Scope

Website Address For This Policy

Related Statutes, Policies, Requirements Or Standards

Contacts

Definitions

Responsibilities

Procedures

Forms Tools/Online Processes

Appendix

POLICY STATEMENT

It is the policy of The University of Texas System Administration (“System Administration”) to take all reasonable steps and to implement all reasonable procedures to detect, prevent and mitigate identity theft, in keeping with federal rules and regulations. In particular, it is the policy of 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 the policy, and to meet the requirements of the Red Flag Rules established by the Federal Trade Commission and other Federal agencies.

RATIONALE

The Federal Trade Commission Red Flag Rules (Rules) require the development and implementation of a written Identity Theft Prevention, Detection and Mitigation Program (“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 System Administration.

This policy provides for the development and implementation of a written Identity Theft Prevention, Detection and Mitigation Program at System Administration to help identify, detect, and respond to patterns, practices, or specific activities – known as “Red Flags” – that could indicate identity theft.

SCOPE

All offices of UT System Administration

WEBSITE ADDRESS FOR THIS POLICY

<http://www.utsystem.edu/policy/policies/int162.html>

RELATED STATUTES, POLICIES, REQUIREMENTS OR STANDARDS

UT System Administration Policies & Standards	Other Policies & Standards
	<p>Fair and Accurate Credit Transactions Act (“FACTA”), 16 CFR 681.2, the Federal Trade Commission’s “Red Flag Rules.” http://www.access.gpo.gov/nara/cfr/waisidx_09/16cfr681_09.html</p> <p>FTC summary of the steps required to comply with the Red Flag Rule at: http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.shtm.</p> <p>FTC summary for health care providers at: http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm</p> <p>FTC “How to Guide for Businesses” 17 pages at: http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf</p> <p>UT System Information Security Incident Reporting Toolkit at: http://www.utsystem.edu/ciso/incident.html</p>

CONTACTS

If you have any questions about UT System Administration Policy INT 162 *Identity Theft Prevention, Detection and Mitigation Program*, contact the following office(s):

Subject	Office Name	Telephone Number	Email/URL
Policy Clarification	UT System Office of Administration	512-499-4209	www.utsystem.edu/administration
	UT System Office of General Counsel	512-499-4462	www.utsystem.edu/ogc
Legal Assistance	UT System Office of General Counsel	512-499-4462	www.utsystem.edu/ogc

DEFINITIONS

Account

Any continuing relationship between 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

Student, Employee, Retired Employee, Patient or other person that has a Covered Account held by or on behalf of System Administration.

Covered Account

An Account System Administration offers or maintains, or that is offered or maintained, by a vendor or other third party on behalf of 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 System Administration offers or maintains for which there is a reasonably foreseeable risk to an Account Holder or to the safety and soundness of 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; 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 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 System Administration's Program.

RESPONSIBILITIES

Chancellor

- Appoints the Responsible Party
- Approves the initial written Identity Theft Program

Vice Chancellor for Administration

- Responsible Party as appointed by the Chancellor
- Develops a written Identity Theft Program
- Encompasses into the Identity Theft Program any existing policies and procedures that promote the purpose of the Program.
- Incorporates information security tools currently available at System Administration, to the extent these tools can assist with implementation of the Program.

Department Head

- Conducts a risk assessment to determine what System Administration accounts, within the responsibility of the department or office, are considered covered accounts, taking into consideration the method System Administration provides to open its accounts; the method System Administration provides to access its accounts; and System Administration's previous experiences with identity theft.

PROCEDURES

1. The Vice Chancellor for Administration 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]**

2. The Vice Chancellor for Administration will set a schedule for Identification of the relevant "Red Flags" associated with the Covered Accounts within each department and office. **[See Appendix A]**
3. The Vice Chancellor for Administration 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 on-going identity theft if possible; and
 - d. mitigate any identity theft that has occurred.**[See Appendices A, B and C]**
4. All 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]**
5. The Vice Chancellor for Administration 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]**
6. The Vice Chancellor for Administration will provide initial training and periodic additional training of all System Administration staff as necessary to implement and enforce the Program effectively. **[See Appendix C]**
7. The Vice Chancellor for Administration 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]**

FORMS AND TOOLS/ONLINE PROCESSES

None

APPENDIX

APPENDIX A: Possible Red Flags in Connection with a Covered Account

Possible Red Flags in connection with establishment of a Covered Account may include:

1. Address discrepancies;
2. Presentation of suspicious documents;
3. Photograph or physical description on the identification that is not consistent with the appearance of the person presenting the identification;
4. Individual Identifying Information provided by a person to establish a Covered Account that is not consistent with other personal identifying information on file with System Administration;
5. Documents provided for identification that appear to have been altered or forged.

Possible Red Flags in connection with an existing account may include:

1. Any unusual or suspicious activity related to Covered Accounts
2. Notification from account holders, law enforcement, or service providers of unusual activity related to a Covered Account
3. Notification from a credit bureau of fraudulent activity regarding a Covered Account
4. A complaint or question from an Account Holder based on the Account Holder's receipt of:
 - a) a bill for another individual
 - b) a bill for a product or service that the Account Holder denies receiving
 - c) a bill from a health care provider that the Account Holder denies patronizing; or
 - d) 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.
5. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the Account Holder.
6. A complaint or question from an Account Holder about the receipt of a collection notice from a bill collector.
7. 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.

8. A complaint or question from an Account Holder about information added to a credit report by a health care provider or third party payor.
9. A dispute of a bill by an Account Holder who claims to be the victim of any type of Identity Theft.
10. 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.
11. A notice or inquiry from an insurance fraud investigator for a private insurance company or a state or federal regulatory or law enforcement agency.
12. A statement from an account holder that a bill or Explanation of Benefits was never received and the address on file is incorrect.

Possible methods of detection of Red Flags include:

1. 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.
2. Requiring multi-factor identification before conducting any transaction relating to a Covered Account with an Account Holder over the telephone.
3. Requiring that on-line transactions come through a secure, password protected portal or in the case of a System Administration employee, a verifiable, secure password protected System Administration e-mail account.
4. 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.
5. Periodically auditing medical records to ensure that treatment is consistent for a single individual.

APPENDIX B: Prevention and Mitigation; Oversight of Third Party Service Providers

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

1. Placing an alert on the record to make all applicable System Administration employees aware that there may be a problem. In some cases, an alert may be requested by the Account Holder.
2. Change any passwords or other authenticating codes related to the Covered Account
3. 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.
4. Correcting erroneous demographic information in the Covered Account record.
5. 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.
6. Closing the Covered Account for the Account Holder and opening a new one with a new account number.
7. Contacting UTPD or other law enforcement agencies upon discovery of possible Identity Theft in connection with a Covered Account.
8. Determining that no response is warranted under the particular circumstances.

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

1. Have a written Program in place that ensures compliance the third party with the Red Flag Rules with respect to all System Administration Covered Accounts; or
2. Adopt and comply with System Administration’s Program with respect to all System Administration Covered Accounts.

APPENDIX C: The University of Texas System Administration Identity Theft Prevention, Detection and Mitigation Program – Approved by the Chancellor on 10.29.09

OVERVIEW

This document constitutes The University of Texas System Administration’s written Identity Theft Prevention, Detection & Mitigation Program (Program) adopted in accordance with INT 162, *Identity Theft Prevention, Detection & Mitigation Policy* and 16 CFR 681.1, the “Red Flags Rule” issued by the Federal Trade Commission pursuant to Section 114 and 315 of the Fair Credit Reporting Act (FACTA) which amended the Fair Credit Reporting Act (FCRA) (Red Flags Rule).

The University of Texas System Administration (System Administration) consists of a variety of offices, some of which are responsible for the central management and coordination of the academic and health institutions; some of which provide centralized services on behalf of The University of Texas System (System) institutions and some of which serve as consultants to System institutions.

System Administration has determined that the following System Administration departments or offices currently house departments that hold Covered Accounts, as defined by INT 162 that require compliance with the Red Flag Rules:

- Accounting and Purchasing Services within Operations and Support Services;
- The Claims and Financial Litigation Section within the Office of General Counsel;
- The Office of Employee Benefits.

Because of the diversity of the missions and services provided by these respective offices and departments, System Administration has determined that each of these offices and departments require customized programs. Accordingly, the Program shall consist of three separate sub-programs.

All three sub-programs shall be overseen by the Vice Chancellor for Administration and will be subject to the same general requirements described in INT 162. As required, System Administration will conduct periodic reviews for Covered Accounts. If additional offices or departments housing Covered Accounts are identified, additional sub-programs may be developed or an existing sub-program may be expanded to include those Covered Accounts.

EFFECTIVE DATE

This program takes effect on November 1, 2009.

RESPONSIBLE PARTY

The Vice Chancellor for Administration is the Responsible Party for the Program. The duties of the Vice Chancellor under the Program include:

- Ensuring that each department or office within System Administration conducts a risk assessment no less than annually to determine whether the department or office has become responsible for a Covered Account;
- Revising the Program to cover all such newly identified Covered Accounts;
- Ensuring that all System Administration employees with responsibility under the Program receive initial and periodic training as necessary to ensure compliance with the Program;
- Reviewing and, as warranted by such reviews, updating the Program to reflect the risks associated with Identity Theft no less than annually;
- Making periodic reports, no less than annually, to the Chancellor to ensure compliance with the program. The first report shall be delivered no later than one year after the date upon which this Program takes effect, or November 1, 2010;
- Any other action required to implement and enforce this Program.

OFFICES AND DEPARTMENTS REQUIRED TO COMPLY; DESIGNATED OFFICE OR DEPARTMENT OFFICIAL

The following departments and/or office hold Covered Accounts that require compliance with the Red Flag Rules and the position within each office or department responsible for oversight are:

- Accounting and Purchasing Services within Operations and Support Services [Director of Accounting and Purchasing Services]
- The Claims and Financial Litigation Section within the Office of General Counsel [Claims and Financial Litigation Section Manager]
- The Office of Employee Benefits [Director of Employee Benefits]

SUB-PROGRAM #1: ACCOUNTING AND PURCHASING SERVICES WITHIN OPERATIONS AND SUPPORT SERVICES

Risk Assessment

A departmental risk assessment is the first step to identify any covered accounts and the potential risk(s) to these accounts. Operations and Support Services - Accounting and Purchasing Services (APS) performed an initial assessment of its business processes and identified the online employee parking program (account) that is subject to inclusion in System Administration's Identity Theft Prevention, Detection and Mitigation Program. To APS's knowledge, there have been no past incidents of attempted or actual identity theft or fraud being perpetrated against the parking account.

APS will conduct a risk assessment as scheduled by the Vice Chancellor for Administration, but no less than annually, to determine whether it offers or maintains covered accounts as described in INT162. The results of the annual risk assessment will be reported to the Vice Chancellor for Administration and will be used to modify System Administration's Identity Theft Prevention, Detection and Mitigation Program.

Definitions

APS incorporates by reference the definitions set forth in INT 165 into its sub-program.

Identification of Red Flags

The responsibility for maintaining an identity theft prevention and mitigation program for the employee parking program lies solely in APS who receives payments on this account and processes refunds in a few situations. The account consists of monthly payroll deductions for employee parking agreements. Employees log in to a secure, password protected portal to setup or update their annual parking agreement. Potential risks within APS's control that could occur would primarily involve attempts by individuals to access the online system to make changes to a parking agreement in order to obtain parking privileges

APS has identified specific red flags that could indicate attempted or actual identity theft or fraud with regard to this account:

- An employee can't log into the on-line parking system with his/her SNAC (password protected);
- A report that a participating employee's SNAC (password protected) has been stolen or otherwise compromised;
- A complaint or question from an employee based on the employee's payroll deduction for parking that the employee denies authorizing;
- The employee's parking permit was stolen or is missing;
- A inquiry from a participating employee that a parking sticker or card was never received; or

- A participating employee claims to be the victim of any type of Identity Theft.

Detecting Red Flags

Methods of detection of Red Flags include:

- Requiring an employee to provide photo identification at each “in person” encounter;
- Requiring that on-line transactions come through a secure, password protected portal or in the case of a System Administration employee, a verifiable, secure password protected System Administration e-mail account; or
- Following up on each payroll deduction inquiry from employees regarding payroll deductions for parking not requested by the employee.

Preventing and Mitigating Identity Theft

When a red flag is detected by an APS employee or who otherwise becomes aware of possible activity that indicates potential or existing fraud or identity theft with regard to the employee parking program shall notify the Director of APS. Upon receipt of such a report, the Director of APS will log the report and gather all available information regarding the transaction, and take any or all action determined to be reasonable under the circumstances to prevent or mitigate identity theft with regard to the employee parking program.

Updating the Program

APS’s identity theft prevention program will be updated to reflect changes in operations and changes in potential risks of identity theft no less than annually by the Director of APS.

Training

APS employees will be trained upon hire and receive annual refresher training on APS’s Identity Theft Prevention Program. The Director of APS is responsible for developing this training and ensuring employees receive this training.

SUB-PROGRAM #2: CLAIMS AND FINANCIAL LITIGATION SECTION WITHIN THE OFFICE OF GENERAL COUNSEL

Risk Assessment

The Claims and Financial Litigation Section within the Office of General Counsel (the Section) has not experienced a situation where attempted or actual fraud or identity theft was perpetrated on a Covered Account, although it is the Section's policy and practice to maintain the privacy and security of the Account Holder information it maintains.

Further minimizing the likelihood of identity theft with regard to the Covered Accounts is the fact that the Account Holders pursued by the Section likely have a poor credit history, and would not be attractive targets for identity theft. Additionally, a large number of the Covered Accounts relate to individuals who are bankrupt or deceased, and would also be unlikely targets of identity theft.

The Section provides services to Institutions that, for the most part, collect, maintain and update the information subsequently used by the Section. As such, the Institutions will be the first line of defense against identity theft.

Suspicious activity that could constitute a red flag indicator of attempted identity theft would be an unusual or unexpected notification of a change of address, an unreasonable request for a complete social security number from a third party regarding a Covered Account, the receipt of correspondence or other contact regarding a Covered Account that references incorrect identifying numbers or demographic information or a dispute by the Account Holder that he did not receive the services for which he is being asked to pay.

With regard to information held or transmitted directly by Section staff, the Section will control the potential for fraud and Identity Theft by maintaining certain safeguards with regard to data relating to Covered Accounts, by training staff to recognize the existence of Red Flags with regard to any transactions with or about a Covered Account, and by training staff to take responsive action when a Red Flag is detected or reported.

Definitions

Account: any *continuing* relationship between an Institution 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: an individual that has a Covered Account held by or on behalf of the Institution.

Covered Account: an Account which has been referred to the Section, which the Institution offers or maintains (or is offered or maintained by a vendor or other third party on behalf of the Institution) primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and any other Account the Institution has referred to the Section which the Institution offers or maintains and for which there is a reasonably foreseeable risk to an Account Holder or to the safety and soundness of the Institution from Identity Theft, including financial, operational, compliance, reputation, or litigation risks. Examples of Covered Accounts include, but are not limited to: student loan accounts, tuition accounts, and medical service accounts.

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 educational 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; IP or other computer identifying address; or telecommunication identifying information or other access device.

Red Flag: a suspicious pattern or practice, or specific activity that indicates the possibility that Identity Theft may occur or is occurring in connection with a Covered Account.

Safeguards Used to Prevent Identity Theft

1. General Safeguards

1.1. Technical Safeguards

The Section relies upon the UT System Office of Technology & Information Services (OTIS) to secure its Covered Account information, which is primarily maintained on UT System servers and desktop hard drives. The Section complies with UT System Administration Policy INT124, Information Resources Acceptable Use and Security Policy. The transmission of information outside of UT System is in compliance with this policy.

1.2. Physical Safeguards

Information regarding a Covered Account is collected, processed, transmitted, distributed and ultimately disposed of with attention to privacy and security. Section staff attempt to use minimal identifying information when corresponding

about a Covered Account outside of UT System, by eliminating the use of unnecessary information, redaction or other methods. Physical folders are maintained in a file room, card access only. Access to Section work areas is restricted based on card access to the elevators. Computers are set to go to password protected screen savers after a short period of time and staff are instructed to manually lock their screen when leaving their work area. After-hours access is limited to authorized employees with electronic pass cards. UT System security further ensures the security of offices during and after hours.

2. Specific Safeguards

2.1. Verification of Address Change Requests

Most address changes are made as a result of a third party verification process, either via notification from the U.S. Postal Service or based on information from a third party subscription service. An Account Holder or authorized agent may also request an address change, which will be made after the Account Holder and/or agent's identity is verified. Address changes may also be made based on information obtained from the Institution.

2.2. Verification Before Providing Social Security Number

Typically, social security numbers will be requested by third parties only as verification of the Account Holder's identity. In this situation, a Section employee would provide the last 4 digits only. The full social security number may be provided to an entitled requestor, i.e. the Account Holder's health insurer, if necessary.

2.3. Receipt of Information with Incorrect Identifying Numbers or Demographic Information

Section employees will investigate discrepancies with the Institution and the Account Holder to clarify, correct or confirm possible suspicious activity if information with incorrect identifying numbers or demographic information is received.

2.4. Disputes regarding Liability for a Covered Account

Section employees verify the validity of a debt with the Institution when the Account Holder disputes liability.

Red Flags

The following have been identified as potential Red Flags based on the risk factors associated with Covered Accounts:

- Any unusual or suspicious activity related to a Covered Account.
- An unverifiable request to change an Account Holder's mailing address.
- Notification from an Account Holder of unusual activity related to a Covered Account.
- Notification from a credit bureau of fraudulent activity regarding a Covered Account.

- A complaint or question from an Account Holder based on the Account Holder's receipt of:
 - a bill for another individual, or
 - a bill for a product or service that the Account Holder denies receiving.
- A statement from an Account Holder that information sent to the Account Holder was never received.
- An improper or unusual request from a third party to disclose an Account Holder's full social security number.
- Receipt of correspondence or other contact regarding a Covered Account that references incorrect identifying numbers or demographic information.
- Notification from the Institution that a Red Flag has occurred with regard to a Covered Account.
- A dispute regarding liability for a Covered Account is received, based on the defense that the Account Holder did not receive the services.
- A complaint or question from an Account Holder about information added to a credit report.
- An Account Holder claims to be the victim of any type of Identity Theft.

Mitigation

A Section employee who encounters a Red Flag situation, or who receives a report from an Institution or others about the existence of a Red Flag, or who is otherwise aware of possible activity that indicates potential or existing fraud or Identity Theft with regard to a Covered Account, shall notify the Section Manager. Upon receipt of such a report, the Section Manager will log the report and gather all available information regarding the transaction, and ensure that any or all of the following actions are taken as applicable:

- Notify the Institution that there may be a problem with the Covered Account and/or placing an alert in applicable records that Identity Theft is believed to be occurring or has occurred with regard to a Covered Account.
- Contact the UT System Office of Police or other law enforcement agencies upon discovery of possible Identity Theft in connection with a Covered Account.
- Ensure that any passwords, PINs, or other authenticating codes that have been compromised relating to the Covered Account are changed.
- Notify 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.
- Correct erroneous information in the Covered Account record resulting from actual or attempted fraud or Identity Theft.
- Conduct 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.
- Temporarily suspend all activity regarding a Covered Account; close a Covered Account.
- Determine that no response is warranted under the particular circumstances.

- Take any other action determined by the Section Manager to be reasonable under the circumstances to prevent or mitigate Identity Theft with regard to the Covered Account.

Documentation

The Section will document all reports of actual or potential Identity Theft and their outcomes for use in periodic evaluation of this Program.

Review and Evaluation of Program and Red Flags

The Section will review this Program as scheduled by the Vice Chancellor for Administration, but no less than annually, and will revise it to reflect changes in operations and changes in potential risks of Identity Theft. The Section will consider in this review:

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

Training

The Section will ensure that all Section employees are aware of this *Program to Prevent, Detect & Mitigate Identity Theft* and receive annual training on all changes made to this Program.

SUB-PROGRAM #3: OFFICE OF EMPLOYEE BENEFITS

Risk Assessment:

The Office of Employee Benefits (OEB) has experienced a minimal history of attempted or actual fraud or identity theft perpetrated on a Covered Account created or maintained by or on behalf of OEB for services, although it has always been the policy and practice to maintain the privacy and security of all information relating to OEB plan and program Participants that is maintained by or on behalf of OEB.

OEB recognizes that insurance coverage, and in particular health care coverage, has become an increasingly important and valuable commodity, and that subsequently information relating to insurance coverage such as member identification numbers, has increasingly become a target for fraud and identity theft. At the same time, OEB's has a duty to ensure the availability of insurance services to benefits-eligible Employees, Retired Employees and their eligible Dependents in a timely and efficient manner. In addition, the Health Information Portability and Accessibility Act (HIPAA) and the HIPAA Privacy regulations, place a duty on health plans to ensure that individuals have reasonably prompt access to their own personal health records.

Many of the services related to the programs and plans provided by OEB are provided by third party vendors that provide or administer the benefits and services available through OEB. Therefore, a great deal, if not most, of the transactions that occur regarding a Participant's Covered Account are conducted by these third party vendors and the information collected and maintained about these transactions are held by the vendors on behalf of OEB.

Given the diverse nature of the plan and programs provided or administered by its third party vendors, OEB has determined that fraud and Identity Theft occurring at the vendor level is best controlled by the vendors. OEB will therefore continue to require by contract that all third party vendors that perform activities in connection with Covered Accounts have written policies and procedures in place designed to detect, prevent and mitigate the risk of fraud and Identity Theft with regard to Covered Accounts and shall provide regular reports to OEB regarding its fraud and Identity Theft and data security Programs, and as necessary require notification on incidents involving OEB program and plan data to OEB to ensure that OEB and/or a Participant can take steps necessary to prevent or mitigate future Identity theft in connection a Covered Account that is not under the control of the third party vendor.

In addition, eligibility for enrollment in OEB plans and programs is based on an individual's status as an Employee or Retired Employee in an Institution or as certain Dependent of an active or deceased Employee or Retired Employee. Determination of that status and the initial creation of a Covered Account with an individual is under the control of the individual Institutions with which the active, deceased or Retired Employees are associated, rather than OEB. OEB merely receives the data used to create

these accounts from the Institutions. Therefore, suspicious activity concerning the creation of a Covered Account that would constitute a Red Flag would normally occur at the Institution and would not be capable of detection or prevention by OEB.

Accordingly, suspicious activity under the direct control of OEB that would constitute a Red Flag centers around existing Covered Account accounts and attempts to obtain or intercept identification cards, debit cards and identifying data involving a Participant in an OEB plan or program that could be used to impersonate a Participant in order to obtain benefits and services available through OEB.

With regard to information held or transmitted directly by OEB staff, OEB shall control the potential for fraud and Identity Theft by maintaining technical and physical safeguard with regard to data relating to Covered Accounts and by training staff to recognize the existence of Red Flags with regard to any transactions with or about a Participant, and to take responsive action when a Red Flag is detected or reported.

Definitions

Covered Account: Any account that OEB maintains to provide to an individual with goods and services under a plan or program or program in return for premium payments made by or on behalf of that individual. For purposes of this policy, an individual's Covered Account includes all of the various programs or plans offered by OEB in which the individual is a Participant and all of the information maintained by or on behalf of OEB pertaining to the Participant.

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 coverage or benefits, to which the individual is not entitled.

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, insurance policy or certificate numbers, alien registration number, passport number, employer or taxpayer identification number, credit/debit/banking account numbers; or enrollment information; (2) claims information or personally identifiable health information; (3) 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.

Institution: A University of Texas System institution, including UT System Administration, whose benefits-eligible Employees and Retired Employees, and the benefits eligible dependents of such employees and retired employees, are entitled to participate in program and plans offered by OEB.

Participant: An Employee, Retired Employee or Surviving Dependent individual who is a Participant in a plan or program offered by OEB and who is the holder of a Covered Account.

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

Technical and Physical Safeguards

Technical Safeguards: OEB complies with U T System Administration INT 124, Information Resources Acceptable Use and Security Policy, at all times. All electronic transfers of OEB data are overseen and performed by OEB's own information technology (IT) staff. OEB's IT staff monitors the security of all of its internal plan and program related systems resources and takes all necessary actions to protect data from unauthorized access. OEB relies upon UT System IT security office to provide network security and administrative software password security according to industry standards in order to protect non-public Participant data that is maintained by UT System outside of OEB. The UT System Administration's Office of Technology Information Services at UT System to provide network security and administrative software password access security according to industry standards in order to protect non-public customer information that is stored on OEB desktop computers and other electronic devices storing non-public customer information. Offsite storage and information processing by third party vendors generally conforms to the same practices as onsite storage, and is safeguarded under the provisions for outside service provide via contract

Physical Safeguards. OEB uses direct personal control or direct supervision to control access to and handling of all non-public customer information when the office is open. All non-public information is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of OEB . Non-public information is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. Conversations concerning non-public information are held in private. Papers with non-public information are mailed via official interagency mail, US mail, or private mail carrier. Electronic files of non-public information are encrypted when transmitted electronically. When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is confidentially destroyed. The OEB offices have restricted access, cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time. After-hours access is limited to authorized employees with electronic pass cards. UT System security further ensures the security of offices after hours. OEB offsite storage and information processing by third party vendors generally conforms to the same practices as onsite storage, and is safeguarded under the provisions for outside service provide via contract.

Verification of Employee Requests to Make Changes to Existing Accounts

All requests for changes to Covered Accounts are verified to have come as having been made by Participant or by an Institution's Benefit Office or an authorized third party vendor.

1. Changes Made Through OEB or an Institution

OEB Staff and Institutions' Benefit Offices must verify the identity of each Participant who requests a change to an existing account, including a Participant's request to change a mailing address or for additional or replacement identification cards, as follows.

1.1. Changes Entered Online.

- a.** OEB accepts online account changes directly from a Participant only through its secure system, MY UT Benefits, which requires Employees to enter a secure password or other secure authenticating information order to access the system.
- b.** OEB will accept change requests, including mailing address changes, from an Institution that were initiated by a Participant through an on line system, only if the system utilized by the institution requires the Participant to enter a secure password or other authenticating code to make changes to their Covered Accounts.

1.2. Employee Submits Change Requests Via Email:

- a.** OEB does not accept change requests directly from Participants via e-mail
- b.** An Institution Benefits Office that by policy allows Employee's to make change requests via e-mail may accept change requests sent through institutional email if the Employee must use a secure Password to access their institutional e-mail program to send the e-mail form.

1.3. Employee Makes Change in Person

- a.** OEB does not accept in-person account changes from Participants.
- b.** An Employee who comes to an Institution's Benefits Office to make changes to an account, must be required to present a valid photo identification (e.g., Employee ID card, passport, or driver's license) for verification unless they are personally known to the Institution's staff member accepting the change request.

1.4. All Other Change Request Methods An Institution that accepts change requests via a non-secure on-line process, telephone, mail, or via an e-mail request that does not come via an Employee's institutional password protected e-mail must verify that the request was made by the Participant by one of the following methods:

- a.** If the request is from an Employee using an non-secure, password protected Institutional e-mail account, by e-mailing the Employee using the Employee's secure, password protected Institutional e-mail address and receiving confirmation that the Employee requested the change via return e-mail from that secure e-mail account;

- b.** If the request is made via telephone, requiring the requestor to verify his or her identity by providing secure information on file for that individual or to correctly answer a pre-selected security question;
- c.** For requests made using any method other than the methods described in section 1.1, 1.2, or 1.3, supra, by sending a written notification of the change request to the mailing address that was on file for the Participant, prior to the receipt of the change request, which notification must contain clear and reasonable instructions for promptly report an incorrect change request, or
- d.** If an Institution has adopted other reasonable policies and procedures as part of an Institution's program to prevent, detect and mitigate Identity Theft (Identity Theft Program) that include processes for validation of address change requests, compliance with the Identity Theft Program.

1.5 Processing of Change Requests

- a.** Only change requests that have been verified as described in section 1.1, 1.2, 1.3, or 1.4, supra will be accepted by OEB.
- b.** OEB will send the changes to the vendor providing or administering the benefit plan on behalf of OEB via secure data transmission.

1.6. Identification of Red Flag and/or Receipt of Unverifiable Requests

- a.** An institution that receives a change request that is accompanied by a possible Red Flag or that is not verifiable for any reason should notify OEB and report and investigate the matter pursuant to the Institution's Identity Theft Program and/or fraud policies. The Institution shall promptly report the outcome of any such investigation to OEB.
- b.** Upon receipt of such a report, OEB will log the report, review the report and if warranted by the report, flag the Participant's account and notify third party vendors as appropriate. If OEB determines that the Red Flag indicates a likely attempt by an unauthorized third party to access a Participant's account information or divert a participant's mail, and the Institution has not done so, OEB may notify the Participant of the attempted access and/or the attempted change.

2. Changes Made Through an OEB Vendor

OEB shall contractually ensure that all vendors authorized by OEB to accept change requests from a Participant, have reasonable policies and procedures in place to prevent, detect and mitigate Identity Theft. If the services provided by a vendor include acceptance of address changes or requests for new or additional identification other cards associated with the account, the vendor's policies and procedures must include reasonable policies and procedures to verify the validity of change request and a process for notifying OEB of unverifiable requests.

Participants' Requests to Access to Claims Data and Other PHI. Participants have a right to access their own claims data and other personal health information (PHI) that is subject to HIPAA pursuant to OEB's HIPAA Privacy Policies. These policies are located in the Employee Office of Employee Administrative Manual at Policy 400, "Health Insurance Portability and Accountability Act". The policies outline the methods to be used for responding to requests for such information by or on behalf of a Participant for access to PHI, including verification requirements.

Red Flags

The following have been identified as potential Red Flags based on the Risk Factors associated with OEB's Covered Accounts:

- Any unusual or suspicious activity related to Covered Accounts.
- A report that a Participant's secure password, PIN or other authenticating item has been lost, stolen, or otherwise compromised.
- An unverifiable request to change a Participant's mailing address.
- Receipt of documents in support of creation of an account, change to an existing account change or a claim for benefit or services that appear to be forged, altered, to identify a person other than the individual one whose behalf the document is presented or otherwise suspicious
- Notification from a Participant, law enforcement, service provider or third party vendors of unusual activity related to a Covered Account
- Notification from a credit bureau of fraudulent activity regarding a Covered Account
- 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 Participant denies receiving
 - a bill from a health care provider that the Participant denies patronizing; or
 - a notice of health plan benefits or other third party payor payments made on behalf of an Participant (such as an Explanation of Benefits) for health services the Participant never received.
- Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the Participant.
- A Participant or third party vendor report that plan or program coverage is denied because benefits have been depleted or a lifetime cap has been reached.
- A dispute of a bill or Explanation of Benefits by a Participant who claims to be the victim of any type of Identity Theft.
- 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 a Participant that a plan or program identification card, debit card, bill or explanation of benefits, was requested by never received.

Mitigation

An OEB employee who encounters or receives a report from an Institution or third party vendor about the existence of a Red Flag or who otherwise aware possible activity that

indicates potential or existing fraud or Identity Theft with regard to a Covered Account shall notify his or her supervisor and the Director of Employee Benefits or the Director's designee ("the Responsible Individual."). Upon receipt of such a report, the Responsible Individual will log the report and gather all available information regarding the transaction, and ensure that any or all of the following actions are taken as applicable:

- Notification of all applicable OEB employees, Institution Benefits Offices and third party vendors that there may be a problem with the Covered Account and/or placing an alert in applicable records that Identity Theft is believed to be occurring or have occurred with regard to the Participant's Covered Account.
- Contacting UT System Office of Police or other law enforcement agencies upon discovery of possible Identity Theft in connection with a Covered Account.
- Ensuring that any passwords, PINs, or other authenticating codes that have been compromised relating to the Covered Account are changed.
- Notifying the Participant of the possible or actual Identity Theft in situations where notification is necessary to or likely to permit the Participant to take action to protect him or herself from the consequences of the Identity Theft.
- Correcting erroneous information in the Covered Account record resulting from actual or attempted fraud or Identity Theft.
- Conducting File extraction—purging the Participant'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.
- Determining that no response is warranted under the particular circumstances.
- Taking any other action determined by the Director or the Director's designee to be reasonable under the circumstances to prevent or mitigate Identity Theft with regard to the Covered Account.

Documentation

OEB will document all reports of actual or potential Identity Theft and their outcomes for use in periodic evaluation of this Policy.

Review and Evaluation of Plan and Red Flags

OEB will review this Policy as scheduled by the Vice Chancellor for Administration, but no less than annually and revise it to reflect changes in operations and changes in potential risks of Identity Theft.

Training

OEB will ensure that all employees are aware of this Identity Theft Detection Policy and receive training on all changes made to this Policy.

Keywords: identity theft, information security, red flag rules, covered accounts
