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.