University of North Texas System Administration
Identity Theft Prevention Program

I. Purpose of the Identity Theft Prevention Program

The Federal Trade Commission ("FTC") requires certain entities, including UNT System Administration (UNTS) to adopt an Identity Theft Prevention Program ("Program") to help prevent Identity Theft. FTC regulations related to Identity Theft prevention are part of the Fair and Accurate Credit Transactions Act and are collectively known as the Red Flags Rule (16 CFR §681). In compliance with the Red Flags Rule, the University of North Texas System Administration's Program is designed to better assist UNT System units and departments in identifying someone who may try to use another individual's identity to gain access to Covered Accounts at UNT System Administration. The System Administration's Program is designed to detect, prevent and mitigate Identity Theft in connection with the opening of a Covered Account or any existing Covered Account.

II. Red Flag Rules Overview

The Red Flags Rule requires users of consumer credit reports, certain creditors and certain card issuers to take various steps to protect consumers from Identity Theft.

Users of credit reports must respond to notices of address discrepancies and take reasonable steps to confirm the accuracy of the address it may have.

A creditor must periodically determine, by conducting a risk assessment, whether it offers or maintains Covered Accounts. Upon identifying any Covered Account(s), the creditor is required to develop and implement a written Identity Theft Prevention Program designed to:

A. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Program;
B. Detect Red Flags;
C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and,
D. Periodically update the program to reflect changes in risks to the account holders or to the safety and soundness of the creditor from Identity Theft.

A card issuer must establish and implement reasonable address verification procedures.

III. Definitions

A. ***"Account"*** means any continuing financial relationship between UNTS and an account holder that permits the account holder to obtain a product or service from UNTS. It may involve the extension of credit for the purchase of a product or service, or a deposit account.

B. ***"Covered Account"*** is any student, faculty, staff, client or patient account that allows payment to be deferred; permits multiple payments or transactions, such as a loan that is billed or payable monthly; or poses a reasonably foreseeable risk of Identity Theft to consumers or businesses. These include, but are not limited to:

- Participation in Federal Perkins Loan Program
- Student Emergency Loan Program
- Payment plans and promissory notes for covered student accounts

C. ***"Identity Theft"*** is a fraud committed or attempted using the identifying information of another person without authorization.

D. ***"Information Resources"*** are the procedures, equipment and software that are employed, designed, built, operated and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

E. ***"Information Security"*** is the protection of information and Information Resources from threats in order to ensure business continuity, minimize business risks, and maximize the ability of the System, System Administration and its Institutions to meet their goals and objectives. Information Security ensures the confidentiality, integrity and availability of Information Resources and information.

F. ***"Personally Identifiable Information"*** means any name or number that may be used, alone or in conjunction with other information, to identify an individual, including, but not limited to:

- Name
- Address
- Telephone Number
- Social Security Number
- Date of Birth
- Government Issued Driver's License Number or Identification Number

- Alien Registration Number
- Government Passport Number
- Employer or Taxpayer Identification Number
- Unique Electronic Identification Number
- Computer's Internet Protocol Address or Routing Code
- UNT System Assigned Student Identification Number
- UNT System Assigned Employee Identification Number

G. ***"Red Flags"*** mean a suspicious pattern, practice or specific activity that indicates the possibility of Identity Theft and that occurs in connection with a Covered Account at UNTS.

IV. Program Oversight

At the University of North Texas System Administration, the Vice Chancellor for Finance is responsible for oversight of the System's Program. The Associate Vice-Chancellor for Finance and Administration or designee is the Program Administrator for the Program and is responsible for developing, implementing, maintaining, and day-to-day operation of the Program. The Program Administrator works with departmental or unit administrators in areas affected by the Red Flags Rule to ensure understanding of and compliance with the Program. The Program Administrator also works in conjunction with the System's Information Security Officer and the appropriate campus' Information Security Officer (as applicable) to address Red Flags and Identity Theft issues related to Information Resources and Information Security.

V. Covered Accounts at the University of North Texas System Administration

The following UNTS units or departments open or administer Covered Accounts and are required to comply with this policy:

- Business Support Services
- Controller's Office
- External Relations (UNT System Building)
- Human Resources
- Payments
- Payroll
- Purchasing
- Student Accounting Services

- Vendor Maintenance
- Any other department, unit, or office at UNTS that opens or administers accounts meeting the definition of Covered Accounts

VI. Identification of Red Flags

In identifying Red Flags related to Covered Accounts and the applicable business procedures of UNTS, UNT System Administration considered the following risk factors: the types of Covered Accounts offered and maintained; the methods provided for opening and accessing each of those accounts; prior experiences with Identity Theft; the size; complexity; nature; and, scope of the institution and its activities. Each of the Red Flags mentioned below may only be applicable to certain Covered Accounts administered by the UNTS.

A. New Covered Accounts:

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

- Address discrepancies
- Presentation of suspicious documents
- Photograph or physical description in the identification document that is not consistent with the appearance of the person presenting the identification
- Personal identifying information that is not consistent with other personal identifying information that is on file with UNTS
- Documents provided for identification that appear to have been altered or forged

B. Existing Covered Accounts:

Possible Red Flags in connection with an existing Covered Account may include:

- Unusual or suspicious activity related to a Covered Account
- Notification from account holders, law enforcement, or service providers of unusual activity related to a Covered Account
- Notification of a problem in connection with a Covered Account from an account holder who claims to be the victim of any type of Identity Theft
- Notification from a credit bureau of fraudulent activity regarding a Covered Account
- Challenge questions used to access a Covered Account are answered incorrectly
- A complaint or question from an account holder based on the receipt of:

i. Bill for another individual
ii. Bill for a product or service the account holder denies receiving
iii. Bill for a health care provider that the account holder denies patronizing

- A complaint or question from an account holder about the receipt of a collection notice from a collection agency when the account holder believes there is no debt
- A statement from an account holder that a bill was never received and the address on file is incorrect

C. Computer Accounts:

Possible Red Flags in connection with a computer account that provides access to or is related to a Covered Account may include:

- Unknown activity related to a computer account or computing services
- Repeat calls to applicable Service Desk to change secret question/secret answer
- Repeat requests to change computing credentials
- Receipt of notices regarding computer accounts or services that an account holder did not authorize
- Log discrepancies
- Social engineering attempts (spam, phishing scams, etc.)
- Unfamiliar user accounts or files
- Modification or deletion of data
- Changes in file or directory permissions

D. Units or departments that administer services for Covered Accounts should identify other relevant Red Flags and incorporate them into this Program.

VII. Red Flag Response:

After detection of a potential Red Flag, the following actions will be taken by UNTS departments or units that open or maintain Covered Accounts when appropriate, given the particular Covered Account at issue and the particular circumstances:

A. Obtain appropriate personal identifying information (e.g., photo identification; date of birth; academic status; user name and password; address; etc.) from the student or individual account holder prior to issuing a new or replacement ID card; opening a Covered Account; or, allowing access to a Covered Account.

B. Provide notification to students and individuals holding Covered Accounts when certain changes to a Covered Account are made, to confirm that change was valid and to provide instruction in the event the change is invalid.

C. Verify suspicious changes made to Covered Accounts that relate to an account holder's identity, administration of the account, and billing and payment information.

D. Whenever an employee identifies a potential Red Flag, the information must be brought to the attention of the supervisor who will investigate the threat to determine the appropriate response and if there has been a breach. Since timing is critical, incidents must be investigated and responded to promptly and contained as quickly as possible. The Department or Unit head will notify the Program Administrator of the occurrence of any Red Flag, specific responses taken pertaining to the Red Flag and any possible breach of a Covered Account. In the event that Information Resources or Information Security may have been compromised, the Information Security Officer for UNTS shall be notified as well. Additional actions by the Program Administrator or the System Administration's Information Security Officer may include notifying and cooperating with the UNTS Office of General Counsel, the applicable campus Police Department and campus Information Security personnel (as applicable), and other campus units as necessary.

VIII. Prevention and Mitigation of Identity Theft

A. Methods to prevent Identity Theft may include, but are not limited to the following actions:

- Requiring each Covered Account Holder to provide photo identification at each "in person" encounter
- Requiring multi-factor identification before conducting any transaction over the phone with the Covered Account Holder relating to a Covered Account
- Requiring an on-line transaction to come through a secure, password protected portal or password protected e-mail account
- Following up on each billing inquiry from a Covered Account Holder when the Covered Account Holder complains of suspicious activity

B. Applicable units or departments should incorporate processes and procedures that address the detection of Red Flags in connection with the opening of Covered Accounts and existing accounts.

C. In addition to the efforts noted above to detect Identity Theft, UNTS personnel involved in the administration of the Covered Accounts will take the following steps, where appropriate and based upon the particular circumstances, to prevent and mitigate occurrences of Identity Theft when a Red Flag is detected:

- Monitor a Covered Account for evidence of Identity Theft
- Contact student(s) and/or individual account holder(s)
- Request additional documentation from the student and/or individual account holder to verify identity
- Change passwords, security codes and other security devices permitting access to the Covered Account
- Reopen a Covered Account with a new account number
- Decline to open a new Covered Account
- Close an existing Covered Account
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances
- Attempt to identify the cause and source of the Red Flag
- Take appropriate steps to modify the applicable process to prevent similar activity in the future
- Notify appropriate UNTS personnel accessing records related to the affected account holder that a Red Flag has been detected

IX. Program Administration

A. Staff Training

The following staff related training offered at UNTS addresses and helps to prevent Identity Theft:

1. ***Red Flags Training*** **-** Training on Identity Theft prevention developed by the Program Administrator's office is designed to assist UNTS departments or units who administer Covered Accounts.

2. ***FERPA Training*** **-** All employees requesting access to student information in EIS (Enterprise Information System) are required to have training in the Family Educational Rights and Privacy Act of 1974, as Amended (FERPA).

3. ***Information Security Training*** **–** UNTS' IT Shared Services (ITSS) is responsible for the Information Security program, which incorporates an Identity Theft

education and awareness component directed towards faculty, staff and students. In addition, training includes methods for detecting and avoiding "social-engineering" techniques (use of inappropriate methods for obtaining protected, sensitive, or confidential information) or phishing scams (a social engineering technique which uses email as a vehicle for obtaining information). Training is offered to faculty and staff online.

4. In addition to the training referenced above, departments and units that administer services related to Covered Accounts should develop and implement plans to effectively train their staff in the identification, detection, prevention and mitigation of the Red Flags identified above that are unique to their specific Covered Accounts. Staff training should be conducted on a regular basis and as necessary under the circumstances related to the administration of the particular Covered Account.

B. Identity Theft Prevention Controls:

The following Identity Theft Prevention controls are in place at UNTS and are used to help prevent Identity Theft:

1. ***UNTS Information Security Handbook for Faculty, Staff, and Students*** - ITSS maintains an Information Security handbook that includes information about protecting information resources. Persons who work with financial, medical, academic, or any other sensitive information are required to read the security handbook and become familiar with the policies and guidelines listed within as a continued effort by UNTS to prevent Identity Theft, as well as FERPA, HIPAA, GLBA, and DMCA violations, and copyright infringement, as appropriate for their position.

2. ***Security Alerts and Notices –*** The Information Security program incorporates a security alert notification component which notifies UNTS' computer support staff when potential threats or risks arise that could cause a negative impact to computing resources or UNTS constituents (e.g., students, faculty, and staff). Alerts can be sent via a variety of means which include email notices and call tracking alert systems.

    - Alerts that are directed to faculty and staff are delivered by one of several means which include support from computer support staff or via administrative announcements. The Associate Vice Chancellor and UNT

System Chief Information Officer send security reminders to faculty and staff regarding their responsibilities for protecting UNTS' computer resources and steps to avoid Identity Theft.

- Alerts that are directed to students are delivered via bulk mail via the student email system.

3. ***Data Security Controls –*** UNTS' critical enterprise computing systems, which house sensitive or confidential data, are protected by strict access controls. Access to these systems (i.e., EIS, Blackboard, MS Office 365, etc.) is provisioned for students, faculty, and staff; however, controls have been established to allow users of the systems to obtain access only to the components and data in which privileges have been granted based on owner defined-controls. Computing access to EIS is removed when employees terminate or retire.

4. ***Software Controls –*** UNTS' enterprise computing systems, which house sensitive data, use encryption to protect data during transmission. In addition, ITSS has data encryption software that allows encryption of sensitive data and helps to prevent unauthorized download or copy of data.

   - UNTS has a site-license for anti-virus software which incorporates anti-spyware. Use of the software reduces the threat of viral infections, computer worms, or Trojan horses that could be used to damage computer systems or collect data from computer systems. Installation and use of anti-virus software is mandatory for all UNTS computer workstations. It is also available to students and can be used for personal home computer use by faculty and staff as provisioned in the software license.

   - UNT System Administration computers are required to be patched and kept-up-to-date with the latest applicable upgrades. The majority of applications can be configured to automatically update and patch software applications. In addition, the windows operating system is configured to enable firewall protection that will prevent unauthorized access to workstations.

5. ***Network Controls –*** UNTS employs several network perimeter controls to prevent unauthorized access to UNTS' computing resources. Controls include a VPN which requires a user-id and password to access computers or applications

on the network, and a firewall that is used to filter against malicious or dangerous traffic.

6. ***Intrusion Detection and Monitoring*** **-** Intrusion detection and prevention systems are in place that detect occurrences of unusual network activity that could be attributed to security threats. These tools trigger alerts if threats are identified. Upon alert, Information Security team staff investigate to determine if incident handling procedures will be initiated.

7. ***Password Controls*** - Password security standards are in place for systems that authenticate against the Account Management System. Standards are in place to ensure that passwords are strong and meet complexity requirements to protect accounts from unauthorized activity.

8. ***Physical Security Controls*** **-** Mandatory Information Security training includes information to assist faculty and staff protect physical resources and data. Protection measures include office and building security, secure use and disposal of confidential documents, and protecting computer equipment and resources.

9. ***Computer System Administration Standards*** **-** Computer System administrators are required to adhere to the system administrator code of ethics, which requires administrators to agree to uphold strict confidentiality and integrity standards when administering computer systems or when they come into contact with data.

10. ***Service Desk*** **-** Registrar Offices associated with UNTS utilize procedures and policies that require mandatory FERPA training prior to obtaining access to any computer system that contains student information. UNT System IT Service Desk staff do not provide personal information to customers. Students who need personal information from their record are referred to the applicable Registrar's Office. Employees who need personal information from their record are referred to Human Resources.

    - Physical security measures are also enabled at the UNTS IT Service Desk. Workstation monitors are not visible from a public vantage point. Customers are never allowed to use workstations that have access to administrative tools. Customer service workstations have limited user rights to help prevent the installation of unwanted programs that may compromise Information Security. Workstations are logged out when not occupied.

- Other protections that are in place at the UNTS IT Service Desk include installation of antivirus software, restricted administrative access to enterprise computing systems is limited to specific workstations. UNTS IT Service Desk staff do not ask customers to provide any personal information through email. Service Desk support requests are received using the IT service management ticketing system.

C. Oversight of Service Providers:

The UNTS contracts with certain third party providers who receive information related to Covered Accounts or who perform an activity in connection with Covered Accounts. UNTS departments and units that maintain Covered Accounts under this Program should take steps necessary to ensure that activities of service providers are conducted in accordance with procedures designed to detect, prevent, and mitigate the risk of Identity Theft. This may include having a written agreement with the third party provider in which the third party provider commits to having a program in place to ensure compliance with the Red Flags Rule.

UNTS contracts or agreements with applicable service providers generally include provisions to protect data and information resources. In addition, UNTS Business Services units, Student Accounting Services, and ITSS are working to establish security, network and payment card industry standards for service providers who conduct business that may involve use of protected data. Standards will include requirements provisioned by the Red Flags Rule, payment card industry data security standard (PCI-DSS), UNT System Information Security Regulations and Texas Department of Information Resources (TX-DIR) Information Security Standards.

D. Reporting:

1. At least annually before the end of the fiscal year, departments and units that maintain Covered Accounts under this Program should report to the Program Administrator, regarding their compliance with this Program. The reporting should address the following elements:

- The department's or unit's identification of Covered Accounts is accurate and up to date, and the department or unit has developed local processes and procedures for addressing Red Flags associated with the Covered Accounts.

- The department or unit has conducted the appropriate training for their staff as necessary and has taken the appropriate steps to ensure any service provider activity is conducted appropriately.

- The department or unit has reported Red Flag occurrences as required.

- Suggested program updates or changes as applicable to the department or unit.

2. The Program Administrator is responsible for conducting an annual Program assessment as described below and providing an annual report to the Vice Chancellor for Finance.

E. Program Assessment and Update:

This Program will be reviewed annually by the Program Administrator. The review will include a risk assessment of the following factors: changes in the methods of Identity Theft; changes in the method of detection; prevention and mitigation of Identity Theft; changes to the Covered Accounts offered and administered by the UNTS; additional units or departments that have become responsible for opening or maintaining Covered Accounts; and, the potential Red Flags that may arise with respect to the Covered Accounts.

The annual risk assessment process will also include an assessment of the Program's effectiveness, significant incidents of Identity Theft, and management's responses. The assessment will consider any changes in risks to students and individual account holders of Identity Theft, findings from the annual departmental reports, and the safety and soundness of the UNTS' identity protection systems. The annual review will include input from the System's Information Security Officer and the applicable locations' Information Security personnel. After the risk assessment is conducted, the Program Administrator will recommend updates to the Identity Theft Prevention Program and the Vice Chancellor for Finance will authorize updates as necessary.

To report a suspected incident of Identity Theft, or if you have questions regarding the UNTS' Identity Theft Protection Program, please contact the Program Administrator at (940) 369-5500.