Policy Chapter:	**Chapter 4 Administration**
Policy Number and Title:	**04.024 Identity Theft Prevention**

I. Policy Statement

The University of North Texas (UNT) will develop, maintain, and update an Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account in accordance with the Federal Trade Commission's (FTC) "Red Flags Rule" (16 C.F.R. § 681). The FTC requires certain entities, including universities, to adopt a 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. In compliance with the Red Flags Rule, UNT's Program is designed to better assist UNT units and departments in identifying someone who may try to use another individual's identity to gain access to covered accounts at UNT.

II. Application of Policy

All employees; and to students, clients, or patients that have a covered account with UNT.

III. Policy Definitions

A. *Account*

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

B. *Covered Account*

"Covered Account," in this policy, means any student, 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:

1. Participation in Federal Perkins Loan Program
2. Student Emergency Loan Program
3. Payment plans and promissory notes for covered student accounts
4. Payment plans for covered employee accounts, such as parking permit or donations

C. *Identity Theft*

"Identity Theft," in this policy, means a fraud committed or attempted using the identifying information of another person without authorization.

D. *Information Resources*

"Information Resources," in this policy, means 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

"Information Security," in this policy, means the protection of information and information resources from threats in order to ensure business continuity, minimize business risks, and maximize the ability of UNT System, System Administration, and Institutions to meet their goals and objectives. Information security ensures the confidentiality, integrity, and availability of information resources and information.

F. Personally Identifiable Information

"Personally Identifiable Information," in this policy, 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:

1. Name
2. Address
3. Telephone Number
4. Social Security Number
5. Date of Birth
6. Government-Issued Driver's License Number or Identification Number
7. Alien Registration Number
8. Government Passport Number
9. Employer or Taxpayer Identification Number
10. Unique Electronic Identification Number
11. Computer's Internet Protocol Address or Routing Code
12. Student Identification Number
13. Employee Identification Number

G. Red Flag

"Red Flag," in this policy, means a suspicious pattern, practice, or specific activity that indicates the possibility of identity theft and that occurs in connection with a covered account at UNT.

IV. Policy Responsibilities

A. Identity Theft Prevention Program

The Vice President for Finance and Administration must establish, maintain, and regularly update a written identity theft prevention program that is in compliance with the FTC's Red Flags Rule.

The program must:

1. identify covered accounts;
2. take into consideration UNT's previous identity theft experiences; and
3. take into consideration the methods UNT uses to open accounts and provide access to them.

B. Oversight and Administration of Identity Theft Prevention Program

The Vice President for Finance and Administration is responsible for oversight of UNT's Program. The Assistant Vice President, Student Accounting is designated as the Program administrator and is responsible for leading development, implementation, operation, and monitoring of the Program. The Program administrator and their team work with departmental or unit administrators in areas affected by the Red Flags Rule to ensure understanding and compliance with the Program. The Program administrator also works in conjunction with the System's Information Security Officer to address Red Flags and Identity Theft issues related to Information Resources and Information Security.

C. Periodic Risk Assessments

UNT departments or units are required to conduct periodic risk assessments to determine if the department or unit has responsibility for covered accounts, which should be recognized by and added to the Program.

D. Departmental/Unit Administrator Responsibility

Departmental or unit administrators in areas affected by the red flags rule are responsible for ensuring compliance with UNT's Program in their department or unit.

E. Identity Theft Prevention Training

The Program administrator must work in conjunction with the System's information security officer to provide identity theft prevention training as needed to ensure understanding of and compliance with the Program by departmental or unit administrators in areas affected by the Red Flags Rule.

F. Annual Departmental/Unit Reports

At least annually before the end of the fiscal year, departments and units that maintain covered accounts are required to make an identity theft prevention report to the Program administrator in accordance with reporting requirements set forth in the written Program.

G. Annual Program Assessment and Report

The Program administrator is responsible for conducting an annual program assessment and providing an annual report to the Vice President for Finance and Administration.

H. Annual Program Review

The Program must be reviewed annually by the Program administrator in accordance with the review requirements set forth in the written Program. The annual review will include input from the System's information security officer and UNT's information security officer (as applicable). After the risk assessment is conducted, the Program administrator will recommend updates to the Identity Theft Prevention Policy and Program. The Vice President for Finance and Administration will authorize updates as necessary, after any policy revisions have been approved by the President in accordance with UNT's standard process for revising policies.

V. References and Cross-References

Fair and Accurate Credit Transactions Act of 2003
16 C.F.R. § 681
UNT System Board of Regents Rule 10.800, Identity Theft
UNT System Information Security Program

VI. Revision History

Policy Contact:	Asst. Vice President, Student Accounting
Approved Date:	10/10/2017
Effective Date:	10/10/2017
Revisions:	11/02/2023, 02/15/2024* * Format only