2040
IDENTITY THEFT PREVENTION PROGRAM

1. General

The College's Identity Theft Prevention Program is designed to detect, prevent, and/or mitigate identity theft in connection with the opening and maintenance of student and employee covered accounts. Covered accounts are accounts that involve or are designed to permit multiple payments or transactions. Examples include, but are not limited to, student financial aid accounts and Bookstore accounts, The Identity Theft Prevention Program defines processes and procedures to guide employees in departments involved with covered accounts in identifying and responding to patterns, practices, or specific activities (Red Flags) that indicate the possible existence of identity theft. Red Flags generally fall within one of the following four categories: suspicious documents, suspicious personal identifying information, suspicious or unusual use of accounts, and/or alerts from others (e.g. customer, identity theft victim, or law enforcement).

Examples of Red Flags include, but are not limited to, documents that appear to be forged or altered, conflicting demographic information, mail returned as "undeliverable" although transactions continue on the account, or a notice or inquiry from a fraud investigator.

This policy applies to the entire College It outlines employee responsibilities, processes, and required training pertaining to Northern's Identity Theft Prevention Program and ensures compliance with the Fair and Accurate Credit Transactions (FACT) Act of 2003 and the accompanying requirement (section 114) to develop and implement a written Identity Theft Prevention Program (16 CFR Part 681, aka "Red Flags Regulation "or "Red Flags Rule").

2. Program Responsibility

2.1. Vice President for Administration and Finance

The Vice President for Administration and Finance is responsible for:

- implementing the Identity Theft Prevention Program,
- conducting periodic reviews of compliance with the Program,
- ensuring compliance with the Program's training requirements, and
- approving material changes to the Program as necessary to address changing identity theft risks.

2.2. Departments

Deans, directors, and departments heads of areas that work with covered accounts are responsible for implementing departmental processes for complying with this policy andensuring that employees responsible for compliance attend required training. Employees in these departments are responsible for:

- complying with the Program,
- identifying relevant Red Flags appropriate for their operations,
- implementing policies and procedures to detect the Red Flags,
- responding appropriately to prevent and mitigate identity theft,
- attending Red Flag training, and

2.3. Information Technology Services (ITS)

The Director of Information Technology shall provide technical support to departments and the Vice President for Administration and Finance.

3. Preventing and Mitigating Identity Theft

3.1. Required Training

Employees involved in student registration, financial aid, student billing and collections, Bookstore sales, and any other area involved with covered accounts must attend training on recognizing and responding to potential identity theft indicators (Red Flags). Every individual currently performing the aforementioned duties must complete this training within one hundred twenty (120) days of the effective date of this policy. All individuals newly performing such duties must complete this training within their first thirty (30) days of starting to perform these duties.

3.2. Identity Verification

To facilitate detection of standard Red Flags, staff will at a minimum take the following steps to obtain and verify the identity of the person.

3.2.1. New Students/Accounts

- Whenever possible, require identifying information (e.g. full name, date of birth, address, and government issued ID, insurance card, etc.).
- When available, verify information with additional identifying documentation such as a credit card, utility bill, medical insurance card, etc.

3.2.3. Existing Accounts

- Verify validity of request for changes of billing address.
- Verify identification of customers before giving out personal information.