UNIVERSITY OF NEBRASKA
UNK
KEARNEY

**Effective:** April 1, 2019
**Last Revised:** *Initial Draft*

**Responsible University Office:**
*Vice Chancellor for Business and Finance*

**Responsible University Administrator:**
*Vice Chancellor for Business and Finance*

**Policy Contact:** *Jon C Watts, wattsjc@unk.edu*

# Red Flag Identity Theft Prevention Policy

**POLICY CONTENTS**



## Scope

The Red Flag Identity Theft Prevention Program (Program) applies to any university activity that extends credit or establishes a transaction account primarily for personal, household or family purposes ("Covered Account"). The Program also applies to departments that can affect the security or integrity of those accounts.

Covered Accounts maintained by the University include but are not limited to the following:

- Child care accounts
- Financial aid/student loan accounts
- Housing accounts
- ID card accounts
- Patient accounts
- Student accounts

The Program the University develops and implements is required to detect, prevent, and mitigate identity theft in connection with the opening of covered

accounts and the administration of existing accounts. The Program must be tailored to the entity's size, complexity and nature of its operations.

## Policy Statement

**Identity Theft Prevention Program**

Accountability is delegated to the Vice Chancellor for Business and Finance to implement Red Flag Identity Theft Prevention Program requirements. At periodic intervals, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment. Periodic reviews will include an assessment of which accounts are covered by the program.

The Program must contain "reasonable policies and procedures" to:

1. Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Update the Program periodically to reflect changes in risks from identify theft to the account holders or to the safety and soundness of the financial institution or creditor.

**Examples of Red Flags**

The University of Nebraska at Kearney shall identify and respond to Red Flags that may indicate potential identity theft. Red flags include, but are not limited to the following:

1. Alerts, notifications or warnings from a consumer reporting agency, including receipt of a fraud or active duty alert, notices of credit freezes, notices of address discrepancies, and receipts of consumer reports showing patterns of activities that are inconsistent with the history and usual pattern of activity of the account holder.

2. Address discrepancies that cannot be explained.

3. Suspicious documents, including: a) photographs or physical descriptions that is inconsistent with the individual presenting the document; b) incomplete, altered, forged, or inauthentic documents; or c) other personal identifying information that is inconsistent with information on file with the University.

4. Complaints or questions from students, guardians, or customers about charges to a covered account for good/services they claim were never received.

5. Suspicious activity related to a Covered Accounts, including; a) unusual use of accounts that have been previously inactive for a lengthy period of time, b) mail being returned as undeliverable although transactions continue to be conducted in connection with the covered account; or c) unauthorized accounts changes or transactions.

6. Notice from customers, victims of identity theft, law enforcement authorities or other individuals regarding possible identity theft in connection with University Covered Accounts.

**Detecting Red Flags**

1. The following actions will be taken as appropriate to confirm the identity of students, patients, and other customers when they open and/or access Covered Accounts.

    a. Obtain appropriate personal identifying information (e.g. photo identification, date of birth, academic status, user name and password, address, etc.) prior to opening or allowing access to a covered account; or prior to issuing a new or replacement ID card.
    b. When certain changes are made to Covered Accounts online, the account holder shall receive notification to confirm the changes is valid.
    c. Verify the accuracy of changes made to Covered Accounts that appear to be suspicious.

2. Information Technology Security Services under the guidance of the Assistant Vice President for NU Information Technology Services and CIO, University of Nebraska at Kearney, shall monitor information systems containing Covered Account information to detect any unusual user activity that could indicate improper access to and/or use of consumer information.

**Responding to Red Flags**

Any staff member encountering a Red Flag shall assess the situation to determine if potential identity theft exists. The assessment may determine that no risk of identity theft is present (i.e. a mistake has occurred, or the occurrence is readily explainable). If, after preliminary investigation, the employee suspects identity theft may have occurred, he/she shall notify the Vice Chancellor for Business and Finance and the Compliance Officer who may activate the UNK Compliance Committee.

The UNK Compliance Committee shall further investigate the matter, and, upon confirmation of identity theft, take the following actions in coordination with the

department managing the Covered Account to mitigate harm, as appropriate, based on the individual circumstances:

1. Notify UNK Police.
2. Notify the covered account holder if the holder is the identity theft victim.
3. Notify the lending institution for student loans or the appropriate University department that awards student aid loans to students.
4. Notify the third party student loan service providers.
5. Notify the campus billing office and third party payers for patient accounts.
6. Notify consumer reporting agency about address discrepancies associated with credit reports received.
7. Notify the State Patrol.
8. File a report with the local police department.
9. Correct any erroneous information associated with the account.
10. Establish Red Flag alerts to notify relevant employees of suspected identify theft (i.e. notes in Covered Account information systems or files, etc.)

The University department responsible for the Covered Account will:

1. Notify the student or individual account holder of the evidence of identity theft and monitor the account for additional fraudulent activity.
2. Request additional information as required to verify identity.
3. Change passwords and security codes as appropriate to further secure access to the account.
4. Reopen a covered account with a new account number, close an existing account, and decline to open a new covered account as appropriate.
5. Attempt to identify the source of the Red Flag and take appropriate steps to prevent additional identity thefts.

## Reason for Policy

The University of Nebraska Red Flag Identity Theft Prevention Program is designed to assist in reducing the risk of identity theft through detection, prevention and mitigation of patterns, practices or activities (“Red Flags”) that might indicate potential identity theft. This policy is intended to comply with the program requirements applicable to the University of Nebraska in the Fair and Accurate Credit Transactions Act (FACTA) at 16 CFR 681.

## Procedures

**Oversight of Service Providers**

The University of Nebraska at Kearney may contract with vendors to provide services related to Covered Accounts. The contracting department shall maintain written certification from the vendor stating it complies with FACTA Red

Flag Rule regulations. The department shall investigate any service provider occurrences indicating a potential lack of compliance, and take any necessary actions to mitigate potential risk.

**Program Education**

All departments managing Covered Accounts shall provide education to current staff members and new hires on this policy and any internal department procedures created to implement it.

**Credit Reports**

Any department ordering credit reports, such as reports on consumers receiving services at the University of Nebraska at Kearney or reports on prospective employees, may receive a Notice of Address Discrepancy from the consumer reporting agency. If such a Notice is received, the administrative unit must compare the information in the consumer report with other address information the individual has provided to confirm the address provided is correct. If the address the individual has provided is correct, the department must notify the consumer reporting agency of the correct address.

**Program Assessment and Reporting**

A Red Flag Identity Theft Prevention Program report shall be forwarded through the Vice Chancellor of Business and Finance to the University of Nebraska Internal Audit Department not later than May 10th of each year for the previous one-year period beginning May 1st through April 30th. The report shall contain:

1. A summary of Red Flag Rule monitoring activities;
2. A description of any identity theft incidents that have occurred and the response to them;
3. Any recommended Red Flag Identity Theft Program Changes.

The University of Nebraska Internal Audit Department shall report information from the administrative units to the Audit Committee of the Board of Regents annually as required by the FACTA regulations. The Board of Regents shall approve material changes to the Red Flag Identity Theft Prevention program.

The Director of Finance will issue an annual reminder to the departments where a higher level of impact could exist for identify theft. These departments are required to complete the Red Flag Identity Theft Prevention Program Annual Attestation form. A summary report of the department incidents involving identify theft is prepared by the Director of Finance and forwarded to the Vice Chancellor for Business and Finance for submission to the Assistant Vice President and Director of Internal Audit.

## Definitions

**Covered account** means

- an account that the University offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and
- any other account that the University offers or maintains for which there is a reasonably foreseeable risk of identity theft to the customer (i.e. students and/or patients) or to the safety and soundness of the University including financial, operational, compliance, reputation, or litigation risks.

**Creditor** means any person who regularly extends, renews, or continues credit, including the University, who accepts multiple payments over time for services rendered.

**Customer** means a student, patient or other individual receiving University services.

**Identify theft** means a fraud committed or attempted using the identifying information of another person without authority

**Identifying information** means any name or number used, alone or in conjunction with any other information, to identify a specific person. Examples include but are not limited to: name, address, telephone number, social security number or taxpayer identification number, alien registration number or passport number, University identification number (NU ID), customer number, date of birth, driver's license number, computer internet protocol (IP) address, banking information and routing number, credit card number and expiration date.

**Notice of an address discrepancy** means a notice that a credit bureau sends to the University when the University has ordered a credit report about a consumer. Mail returned because of improper address is not a notice under this policy.

**Red Flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

**Service provider** means a person that provides a service directly to the University related to a covered account.

## Additional Contacts

| *Subject* | *Contact* | *Phone* | *Email* |
|---|---|---|---|
| **Chief Compliance Officer** | **Mary Chinnock Petroski** | **(308) 865-8400** | **petroskimj@unk.edu** |
| **Assistant VP for NU Information Technology Services and CIO, UNK** | **Deb Schroeder** | **(308) 865-8950** | **dschroeder@nebraska.edu** |

| | | | |
|---|---|---|---|
| | | | |

## Forms

Red Flag Identity Theft Prevention Program Annual Attestation Form

Red Flag Annual Attestation Form.pd

## Related Information

Fair and Accurate Credit Transactions Act (FACTA) at 16 CFR 681

Regents Policy 6.6.12, Red Flag Identity Theft Prevention

## History

This policy replaces current policy located at Business and Finance Policy and Procedures