RED FLAG IDENTITY THEFT PREVENTION PROGRAM

Basis for Policy

Regents Policy 6.6.12, Red Flag Identity Theft Prevention Program; UNMC Policy No. 6055, Fraud (https://wiki.unmc.edu/index.php/Fraud/).

Purpose

The University of Nebraska Medical Center Red Flag Identity Theft Prevention Program is designed to reduce the risk of identity theft through detection, prevention and mitigation of patterns, practices or activities related to covered accounts ("Red Flags") that could be indicative of potential identity theft. The Fair and Accurate Credit Transactions Act (FACTA) contains program requirements at 16 CFR 681. The Vice Chancellor for Business and Finance is responsible for implementing the Red Flag Identity Theft Prevention Program and has delegated day-to-day management to the Compliance Officer.

Definitions

1. *Covered Account* means
   - an account that UNMC 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 UNMC offers or maintains for which there is a reasonably foreseeable risk of identity theft to the customer (i.e. students and/or patients).
2. *Creditor* means any person or organization that extends, renews, or continues credit, including UNMC, who accepts multiple payments over time for services rendered.
3. *Customer* means a student, patient or other individual receiving UNMC services.
4. *Identity theft* means fraud that involves stealing money or getting other benefits by using the identifying information of another person.
5. *Notice of an address discrepancy* means a notice that a credit bureau sends to UNMC when UNMC has ordered a credit report about a consumer. Mail returned because of improper address is not a Notice under this policy.
6. *Red flag* means a pattern, practice or specific activity that could indicate identity theft.
7. *Service Provider* means a vendor that provides services directly to UNMC related to Covered Accounts.

Covered Accounts

Covered accounts maintained by UNMC include but are not limited to the following:

1. Student loans
2. Student accounts
3. Patient accounts

Identifying Red Flags

UNMC shall identify and respond to Red Flags which 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 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:
   - photographs or physical descriptions that are inconsistent with the individual presenting the document;
   - incomplete, altered, forged, or inauthentic documents; or
   - other personal identifying information that is inconsistent with information on file with the University.
4. Complaints or questions from customers about charges to a covered account for goods/services they claim were never received.
5. Suspicious activity related to a Covered Account, including:
   - unusual use of accounts that have been previously inactive for a lengthy period of time,
   - mail being returned as undeliverable although transactions continue to be conducted in connection with the covered account;
   - unauthorized account changes or transactions.
6. Notice from customers, victims of identity theft, law enforcement authorities or other individuals regarding possible identity theft in connection with UNMC Covered Accounts.

Detecting Red Flags

1. The following actions will be taken as appropriate to confirm the identity of customers when they open and/or access Covered Accounts:
   - 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.
   - When certain changes are made to Covered Accounts online, the account holder shall receive notification to confirm the change is valid.
   - Verify the accuracy of changes made to Covered Accounts that appear to be suspicious.
2. Information systems containing Covered Account information shall be monitored by the appointed information system custodian/ administrator 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 Compliance Officer at 402-559-9576 or 402-559-6767.

The Compliance Officer shall further investigate the matter, implementing the Information Security Incident Reporting and Response and/or the Privacy Incident Response Plan Procedures as appropriate. If identity theft is confirmed, the following actions will be taken in coordination with the department managing the Covered Account to mitigate harm, as appropriate, based on the individual circumstances:

1. Notify campus security
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 UNMC department that awards student aid loans to students/third party student loan service providers
4. Notify the campus billing office and third party payers for patient accounts
5. Notify consumer reporting agency about address discrepancies associated with credit reports received
6. Notify the State Patrol
7. File a report with the local police department
8. Correct any erroneous information associated with the account. For patients, notify the Health Information Management Department Manager of Information Logistics so medical information can be adjusted if necessary.
9. Establish Red Flag alerts to notify relevant employees of suspected identity theft (i.e. notes in Covered Account information systems or files, etc.)
10. Request additional information as required to verify identity
11. Change passwords and security codes as appropriate to further secure access to the account.
12. Reopen a covered account with a new account number, close an existing account, and decline to open a new covered account as appropriate
13. Attempt to identify the source of the Red Flag and take appropriate steps to prevent additional identity thefts

Oversight of Service Providers

UNMC 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.

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 April 1st through March 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; and
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.

Additional Information

- Chief Compliance Officer (sarah.glodencarlson@unmc.edu), 402-559-9576 or 402-559-6767
- UNMC Policy No. 6055, Fraud (https://wiki.unmc.edu/index.php/Fraud/)
- Regents Policy 6.6.12, Red Flag Identity Theft Prevention Program