Red Flag Rules
Information and Training

What are Red Flag Rules?

The Red Flag Rules:

- Are enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration.
- Set out how certain businesses and organizations must develop, implement and administer their Identity Theft Prevention Program.
- These rules have been in effect since January 1, 2008.

"As many as nine million Americans have their identities stolen each year. Identity thieves may drain their accounts, damage their credit, and even endanger their medical treatment."

-Federal Trade Commission, "Fighting Fraud with the Red Flag Rule"

Who Must Comply With these Rules?

Financial Institutions and Creditors must comply.

- Although UNM is not a financial institution, we are a creditor because we, “regularly defer payment for goods or services or provide goods or services and bill customers later.” (Ever get a bill from the Bursar’s Office?)
- The definition further describes “covered accounts.” These are accounts where there maybe a “foreseeable risk of identity theft.” This is particularly true if the account can accessed remotely, such a through the Internet or telephone.
- In thinking about identity theft, we must go beyond “accounts” at UNM and think about things like, Admissions, Financial Aid, Employment Applications. All can send up a “red flag.”

UNM Covered Accounts Include

- But are not limited to:
  - Student Accounts Receivable
  - LoboCa$h
  - Bookstore Accounts
  - Patient Accounts
  - Employee Accounts Receivable and Employment Records
  - Any Department Offering Goods/Services and Accepting Payment at a Later Date

Compliance is a Four-Step Process

- Step 1: Identify Relevant Red Flags
- Step 2: Detect Red Flags
- Step 3: Prevent and Mitigate Identity Theft
- Step 4: Update your Program

Let’s Go Over Each Step . . . .

Each Department is Unique

The following slides are guidelines for identifying, detecting and mitigating identity theft. Each department has unique circumstances and “accounts.”

Each department dealing with covered accounts must develop their own program for dealing with identity theft. That program must be reviewed and updated periodically.

Step 1: Identify Red Flags

There are five different categories for identifying red flags:

1. Notifications and Warnings from Credit Reporting Agencies
2. Suspicious Documents
3. Suspicious Personal Identifying Information
4. Suspicious Covered Account Activity or Unusual Use of Account
5. Alerts from Others

Step 1: Identify (continued)

Category 1: Notifications and Warnings from Credit Reporting Agencies:

Most UNM Departments do not request credit reports on a regular basis.

If your department does use credit reports for whatever reason, Red Flags may include:

1. Report of fraud accompanying a credit report;
2. Notice from a credit agency of a credit freeze;
3. Notice from a credit agency of an “active duty alert”;
4. Receipt of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity inconsistent with an applicant’s usual pattern or activity.

Step 1: Identify (continued)

Category 2: Suspicious Documents:

Almost all UNM departments with covered accounts work with some form of documentation. These documents may include employment applications, applications for admissions, taxation and revenue documentation and change of address request. Red flags include:

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student/employee information; and
4. Application that appears to have been altered or forged.

Step 1: Identify (continued)

Category 3: Suspicious Personal Identifying Information:

When dealing with individuals at UNM, proper identifying information is needed. This may include a Lobo ID, driver's license or passport. On the phone, employees should verify birth date or other personal information. This doesn't stop with student contact as described below:

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. The social security number has not been issued or is listed on the Social Security Administration's Death Master File;
3. A person fails to provide complete personal identifying information on an application when reminded to do so; and
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).

Step 1: Identify (continued)

Category 4: Suspicious Account Activity or Unusual Use of Account

Any of the following should be considered a Red Flag. Use your own judgment. Is there anything else specific to your department that may cause concern? For example, a student charging only electronic devices (e.g. iPods or laptop computer) to their UNM Bookstore account.

1. Change of address on account followed by a request to change the student's name;
2. Payments stop on an otherwise up-to-date account;
3. Mail sent to a student is repeatedly undeliverable although there is account activity;
4. Notice to UNM that the student is not receiving any UNM mail;
5. Notice to UNM that the account has unauthorized activity;
6. Unauthorized access to or use of student account information; and
7. Breach in UNM's computer system security.

Step 1: Identify (continued)

Category 5: Alerts from Others:

An obvious Red Flag occurs whenever notice is given to UNM from a student, identity theft victim, law enforcement agency or other person that UNM has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Once you've identified what constitutes a possible Red Flag, what's the next step?

Step 2: Detect Red Flags

Now that your department knows what a Red Flag looks like, it's time to come up with procedures to detect Red Flags in your own area. Two areas of particular concern are:

1. Obtaining identifying information about, and verifying the identity of a person opening/maintaining a covered account. This is as simple as requesting a picture ID anytime a student transacts business with your department. And, in the case of issuing a LoboCard to a new or existing student, requesting additional photo identification and verifying information such as address and date of birth.
2. Authenticating customers (e.g. requiring a logon ID and password if online or verifying birthday and/or class schedule by phone), monitoring transactions and verifying the validity of change of address requests. For example, the Bursar's Office will not change account addresses. Students are directed to do this online as a logon ID and password are required for authentication.

Step 3: Prevent and Mitigate Identity Theft

In the event UNM personnel detect any identified Red Flags, these individuals should discuss the situation with his or her supervisor who will take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate:

-Continue to monitor an account for evidence of identity theft.

-Contact the student or applicant.

-Change passwords or other security devices that permit access to the account.

-Not open a new account/admit student.

-Provide student with a new ID number.

-Notify the department Dean or Director.

-Notify the Program Administrator for determination of the appropriate steps to take.

-Notify law enforcement.

-Determine that no response is warranted under the particular circumstances.

Step 3: Prevent and Mitigate Identity Theft (continued)

Protect Student/Employee Identifying Information:

-Ensure that the UNM website is secure or provide clear notice that the website is not secure.

-Ensure complete destruction of paper documents and computer files containing student account information when a decision is made to no longer maintain such information.

-Ensure office computers with access to account information are password protected.

-Avoid use of Social Security Numbers.

-Ensure computer virus protection is up-to-date.

-Require and keep only the kinds of student information that are necessary for University purposes.

Step 4: Update the Program

UNM UBPPM Policy 2040, *Identity Theft Prevention Program,* states, “Deans, directors and department heads of areas that work with covered accounts are responsible for implementing departmental processes for complying with this policy . . . “

Each department working with covered accounts must implement policies and procedures related to identifying, detecting, mitigating and preventing identity theft.

In addition, a detailed report of all incidents of identity theft and “suspicious behavior that may be related to identity theft” must be submitted to the Office of the Vice President for HSC/UNM Finance and University Controller.

Our environment changes constantly. Technological advances and the ability to conduct most business online makes it imperative that individual departmental policies and procedures be reviewed and updated periodically.

Know your environment.

Know your customers.

Know your risk.

Example of a Red Flag Incident

Mary works in the Bursar's Office. She receives a call one day from a student requesting information on a refund check that should have been mailed to her weeks ago. Mary, according to Bursar's procedures, asks the student to verify her birth date and asks her what courses she is taking the current semester. The student provides information that matches the system data.

Mary determines that a refund check was issued two weeks ago. She looks up the mailing address and asks the student to verify this address. The two addresses do not match. The address the student provides was "inactivated" when a new address was entered. Upon further investigation, the address was not changed online by the student but by another department at UNM.

Mary sees a Red Flag. She informs the student she will look into the matter further and someone will call her back. Immediately she reports the Red Flag to her supervisor. Her supervisor looks into the matter and finds that the check was cashed but the signature on the copy of the cancelled check does not match any other signatures on prior checks or other UNM documentation signed by the student.

Example of a Red Flag Incident (continued)

Mary's supervisor determines that this is definitely a possible identity theft situation. She contacts the student, prepares a written report and contacts the UNM Police Department. The UNM Police Department will contact the potential identity theft victim (student) and investigate fully.

This incident and any others that occur will be included on the periodic report submitted to the Office of the Vice President for HSC/UNM Finance and University Controller.

Further Information:

- The department that changed the address should have asked for other documentation showing the new address and a photo ID as verification of the identity of the individual and evidence of a valid address. Or, the student should have been directed to change the address online with a logon ID and password.

- The student will be issued another check. Because the signature is not hers, an affidavit must be completed and submitted to the bank, but she will receive a replacement check.

Where Can I Get More Information?

UNM UBPPM Policy 2040 – Identity Theft Prevention Program:

http://policy.unm.edu/university-policies/2000/2040.html

UNM UBPPM Policy 7200 - Cash Management Policy:

https://policy.unm.edu/university-policies/7000/7200.html

Federal Trade Commission's (FTC) Red Flags Rule Website:

http://ftc.gov/redflagsrule

National Association of College and University Business Officers (NACUBO) site containing links to both NACUBO Resources and FTC Resources:

http://www.nacubo.org/Initiatives/FTC_Red_Flags_Rule.html