University of Minnesota Identity Theft Prevention Program: Red Flags Rule

Detecting, Preventing, and Mitigating Identity Theft

This presentation was adapted with permission from the University of Florida and MnSCU.
The Goals of This Training

- To define commonly used terms related to Identity Theft.
- To explain the federal rules intended to detect, prevent and mitigate Identity Theft.
- To help you identify if you must comply with one or more sections of the Red Flags Rule.
- To assist you in creating unit-specific procedures that will comply with the Identity Theft Prevention Program approved by the Board of Regents.
A warning signal. Something that demands attention or provokes an irritated reaction.
Identity Theft – Red Flag

A pattern, practice, or specific activity that indicates the possible existence of identity theft.
The Red Flags Rule

• The Red Flags Rule applies to financial institutions and creditors that offer or maintain covered accounts.

• The Rule requires the implementation of a written *Identity Theft Prevention Program*.

• The University of Minnesota’s Program is available at the [Controller’s Office Red Flags Rule website](#).
The University of Minnesota falls within the scope of the **Red Flags Rule** because we act as a “creditor” or “financial institution” by:

- Regularly extending, renewing, or continuing credit; arranging for credit or acting as an assignee of an original creditor;
- Issuing credit or debit cards.

Simply accepting credit cards as a form of payment does not make you a “creditor” under the Red Flags Rule. Likewise, you are not a “creditor” if you advance funds for expenses incidental to a service such as billing for medical, dental, legal, or veterinary services.

But if you offer a debit or credit card, arrange credit for customers, or regularly and in the ordinary course of business advance funds based on an obligation to repay the funds, you are a “creditor” under the law.
Covered Accounts

• The Rule’s goal is to detect, prevent, and mitigate identity theft in certain “covered accounts”.

• A “covered account” is any account that a college or major administrative unit offers or maintains:
  – Primarily for personal, family, or household purposes that permits multiple payments or transactions, or
  – For which there is a reasonably foreseeable risk of identity theft.

• The University must periodically assess what areas contain “covered accounts”.

The Rule…

… is actually two different but related rules. Review each rule to determine if one or more applies to your unit.

- (681.1) **Creditors** holding “Covered Accounts”
- (681.2) Issuers of **Credit or Debit Cards, or Stored Value Cards**
Creditors with Covered Accounts

• (681.1) Creditors holding “covered accounts” must develop and implement written procedures designed to detect, prevent and mitigate identity theft in connection with new and existing accounts.

• This section applies to areas of the University that issue credit in the form of financial aid and other student loans.

• Section 681.1 is the “Red Flags” section of the Red Flags Rule.

* Refer to the University’s Identity Theft Prevention Program and support materials at the Controller’s Office website for specific compliance requirements.
Debit and Credit Card Issuers

• (681.2) Debit and credit card issuers must develop reasonable policies and procedures to assess the validity of a request for change of address that is followed closely by a request for an additional or replacement card.

• This section applies to the U Card (including Gopher Gold), payroll deduct cards, and Care Credit cards.

* Refer to the University’s Identity Theft Prevention Program and support materials at the Controller’s Office website for specific compliance requirements.
Identifying Red Flags

❖ A Red Flag, or a situation closely resembling one, should be investigated.

❖ Potential indications of fraud include:
  • Alerts, notifications, or other warnings from credit agencies.
  • Suspicious documents or personal identifying information.
  • Unusual or suspicious account activities.
  • Notices from customers, victims of identity theft, law enforcement authorities, or others.
Alerts, Notifications, and Warnings

- Watch for these notices from consumer reporting agencies, service providers, or fraud detection services:
  - A notice of address discrepancy;
  - An active duty alert or a fraud alert included with a consumer report; or
  - A notice of credit freeze in response to a request for a consumer report.

Identify a procedure for appropriate responses to address discrepancy notices.
Suspicious Documents

• Identification documents that appear to have been altered or forged.
• The photograph or physical description on an ID that doesn’t match the customer presenting it.
• Information on the identification that is inconsistent with other information provided or readily accessible, such as a signature card or a recent check.
• An application or document that appears to have been destroyed and reassembled.
• **Personal Identifying Information** (PII) provided is inconsistent with PII that is on file, or when compared to external sources. Examples would be:

  – The *address does not match* any address in the consumer report;
  – The SSN has not been issued or is listed on the Social Security Administration’s *Death Master File*;
  – There is a *lack of correlation* between the SSN range and date of birth.
Fraudulent Personal Information

• Personally identifiable information provided is associated with **known fraudulent activity**, or is of a type commonly associated with fraudulent activity. For example,
  – The address on a document is the same as the address provided on a **known fraudulent document**;
  – The address on a document is **fictitious, a mail drop, or a prison**;
  – The phone number is **invalid** or associated with an answering service.
Just how suspicious is….?

• ..a SSN provided for an account is the same as one provided by another person for a different account?
  – How would you know?
• …the person opening a Covered Account fails to provide all the required personal identifying information on an application and then doesn’t respond to notices that the application is incomplete?
  – What do you do next?
• …a person requesting access to a Covered Account cannot answer the security questions (mother’s maiden name, pet’s name, etc.)?
  – How do you handle this?
Looking Below the Surface

• Sometimes fraudulent activity is not that obvious.

• Be ready to respond to situations like these:
  – Mail sent to the account-holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Covered Account.
  – The institution is notified that a customer is not receiving paper account statements, even though they are being mailed and not returned.
On the Other Hand…

- Even if the problem is obvious, be sure you know the procedure to follow in situations such as these:
  - You receive a notice regarding possible identity theft in connection with Covered Accounts held by your unit.
  - You are notified that your department has opened a fraudulent account for a person engaged in identity theft.
Responding to Red Flags

Report **known and suspected** fraudulent activity immediately to protect the customer and the University from damages and loss:

- Take appropriate action.
- Gather all related documentation.
- Complete an incident report with a complete description of the situation.
- Send the report to your supervisor.
- Add the incident to an incident log.
- Also…in certain situations additional cooperation and assistance may be required to notify appropriate law enforcement, determine the extent of liability, and notifying the customer.
Tips to Keep Data Safe

✓ Always keep private information in a secured area.
✓ Destroy paper according to University Guidelines.
✓ Use strong passwords.
✓ Know where your data is.
✓ Keep strict controls on data access.
✓ Use secure file servers to store private data; limit "C" drive storage.
✓ Use a Virtual Private Network (VPN) to connect from off-campus.
✓ Never use public computing devices to work with private information.
✓ Never use email for private data unless the each part of the process is known to be secure.
Thank you for reading this presentation!

- The University of Minnesota’s *Identity Theft Prevention Program* and training materials are available on the [Controller’s Office Red Flags Rule website](https://controller.umn.edu/).

- Contact the Controller’s Office at [controller@umn.edu](mailto:controller@umn.edu) or (612) 624-1617.

- Contact [abuse@umn.edu](mailto:abuse@umn.edu) or 1-HELP (1-4357) for computer security issues.


This presentation was adapted with permission from the University of Florida and MnSCU.