THE RED FLAG RULE

Understanding our requirements and ensuring compliance
The FTC = Federal Trade Commission

The FTC issued the Red Flag Rule as part of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Sections 114 and 315.

Final regulations issued November 9, 2007, 16 CFR 681.1, 681.2, and 681.3
The Red Flag Rule supplements existing legislation aimed at detecting, and preventing identity theft.

Applies to “financial institutions” and “creditors” with “covered accounts”.

Sets out how affected institutions/accounts must develop, implement, and administer their Identity Theft Prevention Programs.

Picks up where data security leaves off.
Dumpster Diving. They rummage through trash looking for bills or other paper with your personal information on it.

Skimming. They steal credit/debit card numbers by using a special storage device when processing your card.

Phishing. They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.

Changing Your Address. They divert your billing statements to another location by completing a change of address form.

Old-Fashioned Stealing. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.

Pretexting. They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.
Under the authority of the Federal Trade Commission (FTC) the new rule requires certain businesses and organizations to:

- Develop
- Implement; and,
- Administer

Identity Theft Prevention Programs
Must include reasonable written policies and procedures to identify the “red flags” of identity theft that may occur in day-to-day operations.

Must be designed to detect the potential “red flags” identified.

Must spell out appropriate actions the organization will take when “red flags” are detected.

Must include appropriate staff training.

Must be re-evaluated periodically to reflect new risks.
WHO MUST COMPLY?

- Determination isn’t based on industry or sector but whether your activities fall within the relevant definitions:
  - “Financial Institution”
  - “Creditor”
  - “Covered account”
WHO MUST COMPLY?

- “Financial Institution”
  - State or national bank, savings and loan, mutual savings bank, credit union or any person that directly or indirectly holds a transaction account belonging to a consumer

- “Creditor”
  - Businesses or organizations that regularly defer payments for goods or services and bill customers later
  - Anyone who regularly participates in decision to extend, renew, or continue credit
  - Includes third-party debt collector
WHO MUST COMPLY?

“Covered Accounts”

- A consumer account offered or maintained, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time.

- Any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers of identity theft.
All campus units that work with “covered accounts” are subject to these regulations.

Examples include any units that offer:
- Deferred payment plans
- Loans
- Other extension of credit
- Or hold other accounts where there is a *foreseeable risk* of identity theft

DETECTING RED FLAGS AT PURDUE
WHAT DOES THE RED FLAGS RULE REQUIRE?

- Affected companies, such as Purdue, must develop and implement **written** identity theft prevention programs to:
  - Identify
  - Detect
  - Mitigate
A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Regulation provides many examples of “Red Flags” and the following categories are outlined in the regulations:
EXAMPLES OF RED FLAGS

- Fraud or Active duty alerts
- Notice of credit freezes
- Address discrepancy
- Activity pattern change
EXAMPLES OF RED FLAGS

- Identification documents appear forged
- Photograph or identification does not agree with the appearance of the applicant
- Provided documentation is inconsistent with the file
Examples of Red Flags

- Inconsistent information or information that matches fraudulent accounts
- A Social Security Number that matches other accounts
- Information that doesn’t match external sources such as an address that does not match the credit report address
EXAMPLES OF RED FLAGS

- New or additional users shortly after a change of address
- Returned mail from an active account
- Fraudulent patterns such as failure to make first or subsequent payments
- Notification of unauthorized charges
EXAMPLES OF RED FLAGS

- Notice from customers, victims of ID theft, or Law Enforcement regarding possible Identity Theft in connection with a customer account
COMPLIANCE: A FOUR STEP PROCESS

1. Identify likely “red flags” in your operations

2. Detect “red flags” in day-to-day operations

3. Prevent and mitigate identity theft
   - Respond appropriately
   - Mitigate the harm done

4. Update your program
   - Conduct periodic risk assessment
   - Educate staff
RESOURCES


- FTC Red Flag site available at http://www.ftc.gov/redflagstrule (This site includes an instructional video)

- Departmental Plan/Controls