UNDERSTANDING RED FLAG REGULATIONS AND ENSURING COMPLIANCE

University of Cincinnati

Red Flags Rule

Protecting Against Identity Fraud

UNIVERSITY OF Cincinnati

Objectives

- Background
  - What is the FTC Red Flags Rule?
  - Why do we need it?
  - Who must comply?
  - Ensure everyone understands what a “Red Flag” is
  - Ensure everyone is clear about their responsibilities for compliance

What is the Red Flags Rule

- The rule supplements existing legislation aimed at 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

What is identity theft?

- Fraudulent use of someone’s personal information
- Impersonating another individual to gain services/benefits/funds/resources
  - Includes medical identity theft
- Serious crime – may wreak havoc on your finances, credit history and reputation

Personally Identifiable Information

Consumers

- First, middle, or last name
- Date of birth
- Address
- Telephone or wireless numbers
- Social Security number
- Maiden name
- Account numbers

Credit card information

- Account number (whole or part)
- Expiration date
- Cardholder name
- Cardholder address

Medical information for any customer

- Doctor names and claims
- Insurance claims
- Prescriptions
- Treatment or diagnoses
- Any related personal medical information

What is a Red Flag?

- 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:
  - Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.
  - Presentation of suspicious documents.
  - Presentation of suspicious personal identifying information.
  - Unusual use of, or other suspicious activity related to, a covered account.
  - Notice from customers, victims of identity theft, or law enforcement

Regulation Requirements

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

Program Elements

Must include policies and procedures to:

- Develop and implement written policies and procedures to identify relevant red flags and incorporate them into the plan and controls
- Train staff
- Detect the potential *red flags* identified
- Define the appropriate actions the organization will take when *red flags* are detected
- Respond appropriately to any red flags that are detected to determine if fraudulent activity has occurred
- Ensure the plan and controls are updated periodically to address changing risks
- Have senior management oversight

Example of Red Flags

- Documents provided for identification appear to have been altered or forged
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- Personal identifying information provided is inconsistent when compared against external information.
- The Social Security number provided is the same as that submitted by others.
- Social Security numbers do not match on all documents.
- The customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
- Personal identifying information provided is not consistent with personal identifying information on file.
- Excessive address changes.
- Unusual number of inquires on the account.
- A student asking for their student number because they lost their ID card.

Who Must Comply?

- Financial Institutions
  - 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
- Creditors
  - 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
- 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*

Four Steps to Compliance

- Identify likely *red flags* in your operations
- Detect *red flags* in day-to-day operations
- Prevent and mitigate identity theft
  - Respond appropriately
  - Mitigate the harm done
- Update your program
  - Conduct periodic risk assessment
  - Educate staff

What To Do When a Red Flag Surfaces?

- Most important - notify your manager immediately
- Gather all related documentation
- Write a description of the situation
- Monitor the account involved
- Contact the customer
- Change passwords if needed
- Notify law enforcement
- Or determine no response is warranted in this case

How Does This Affect UC?

- All campus units that work with “covered accounts” are subject to these regulations
- Examples include any units that offer:
  - Deferred payment plans
  - Direct lending
  - Other extension of credit
  - Or hold other accounts where there is a *foreseeable risk of identity theft*

UNIVERSITY OF Cincinnati

Examples of Impacted Departments

- Office of the Bursar
- Student Financial Aid
- Human Resources
- Campus Services
- Academic Health Center

Support

UCIT Office of Information Security provides support by:

- offering/conducting security risks assessments
- communicating through this training program
- providing guidelines for secure computer data
- providing resource and educational materials
- providing security tools and software
- providing support for safeguard failure response

Every Department Plays a Role

Each department:

- is required to have a security policy
- is responsible for training staff
- needs to be aware of *red flags*
- needs to assure that staff are familiar with the web sites for safeguarding information of these three types:
  - administrative
  - technical
  - physical

Resources

- Available resources:

  Many policies, procedures and resources are available that support our efforts to protect non-public personal information. A list of related resources can be found on the UCIT Information Security web page: http://www.uc.edu/infosec.html