THE RED FLAGS RULE

Detecting, Preventing, and Mitigating Identity Theft

Training for Ball State University's Identity Theft Protection Program

What is the Red Flag Rule?

- Congress passed the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") which amended the Fair Credit Reporting Act ("FRCA") to require the Federal Trade Commission and other federal agencies to adopt identity theft red flags rules and guidelines
- Pursuant to this legislation, the Federal Trade Commission issued regulations known as the ***Red Flag Rules***, 16 CRF § 681.1 et seq.
- Generally, the Red Flags Rules require financial institutions and creditors that maintain ***covered accounts*** to develop and implement a written Identity Theft Prevention Program.

Why must Ball State comply with the Red Flag Rules?

- The ***Red Flag Rules*** require “financial institutions” and “creditors” to conduct periodic risk assessment.
- While Ball State may not be a financial institution in the typical sense, under the law this determination is not based on the industry or sector of an organization, but rather on whether an organization’s business activities fall within the relevant definitions.

Why is Ball State a “creditor”?

- The ***Red Flags Rule*** defines “creditor” based on conduct such as:
  - Regularly deferring payments for goods or services and billing customers later. Some examples are allowing students to pay on installment plans and employees to use payroll deductions for services such as parking or recreation passes.
  - Arranging and administering Perkins loans and advancing funds through university student loans.
  - Reporting information to credit reporting agencies.

Covered Accounts

- Because Ball State qualifies as a "creditor," it must determine what qualifies as a "***covered account***."
- A covered account is any account that a creditor offers or maintains primarily for personal, family, or household purposes that is designed to permit multiple payments or transactions.
- Further, a covered account can be any other account that Ball State offers for which there is a *reasonably foreseeable risk* of identity theft.
  - Think beyond financial accounts - this may include student files in Admissions or employment applications

Examples of Covered Accounts

- Employee payroll deductions
  - Parking Services
  - Recreation Memberships and Fitness Passes
- Installment Payment Plans
- Meal Plans, Cardinal Cash and Dining Plus Accounts
- Perkins and University Loans
- Fines or fees from Parking or University Libraries
- Background checks or credit reports used for hiring decisions and students enrolled in certain programs

Ball State's Red Flags Policy

- Identify areas of exposure to identity theft and what types of events within those areas could be interpreted as a Red Flag.
- http://cms.bsu.edu/about/administrativeoffices/legal/identitytheft
- The goal of the policy and this training is to **reduce the exposure of financial and personal loss to both the individual and the University**.

How Do You Comply?

Step #1: Identify what constitutes a “Red Flag”

Step #2: Detect Red Flags in accounts and operations

Step #3: Prevent and Mitigate Identify Theft

Step #4: Update and Administer the Program

Step #1: What constitutes a Red Flag?

- Red Flags are potential patterns, practices, or activities indicating the possibility of identity theft.
- In simple terms, a Red Flag is an indication that a fraudulent transaction or event could be occurring as a result of identity theft.
- Red Flags come in five general categories
  - Notifications and Warnings from Consumer Reporting Agencies
  - Suspicious Documents
  - Suspicious Personal Identifying Information
  - Suspicious Covered Account Activity
  - Alerts from Others

Step #1: Notifications and Warnings from Consumer Reporting Agencies (cont.)

- Fraud alert included with a consumer credit report from a credit bureau
- Notice of credit freeze
- Notice of address discrepancy
- Report of unusual credit activity, such as an increased number of accounts or inquiries

Step #1: Suspicious Documents (cont.)

- Documents provided for identification appear to be altered or forged
- Photograph on ID does not match the appearance of the individual
- Information on the ID does not match the information provided by the person opening the account
- Application appears forged, altered, or destroyed and reassembled
- Signatures on multiple documents do not match

Step #1: Suspicious Personal Identifying Information (cont.)

- Information on the ID does not match any address in the consumer report
- Social Security Number (SSN) has not been issued or appears on the Social Security Administration's Death Master File
- Correlation between the SSN provided and the range for the date of birth
- Duplicate SSN is provided that matches one submitted by another person or another customer with an existing account
- Suspicious address is provided, such as a mail drop or prison
- Duplicate addresses or phone numbers that match others, or have been supplied by a large number of applicants
- The person opening the account is unable to supply identifying information when told the application is incomplete
- Applicant's personal information is inconsistent with information already on file
- The applicant or existing customer is unable to correctly answer challenge or security questions

Step #1: Suspicious Covered Account Activity (cont.)

- Shortly after a change of address on an account, you receive a request for additional users
- Drastic change in payment patterns, use of available credit, or spending patterns
- An inactive account suddenly has a lot of unusual activity
- Mail that has been sent to the customer is repeatedly returned as undeliverable despite continued transactions on the account
- You are notified that a customer is not receiving his or her account statements
- You are notified of unauthorized charges or transactions on a customer's account

Step #1: Alerts from Others (cont.)

- The customer notifies you that he or she has been a victim of identity theft
- You receive a notification from a third party (such as law enforcement or an attorney) that there is a fraudulent account being used at the University by a person engaged in identify theft
- You receive an alert that the security system or procedures have been compromised

Step #2: Detect Red Flags

- Once you know what a Red Flag looks like, your department must have procedures to detect Red Flags.
- Use reasonable procedures to verify the identity of the person you are dealing with
  - These procedures may vary depending on the nature of the account and the transaction or information requested.
  - Obtain identifying information about and verify the identity of a person opening/maintaining a covered account.
- For in-person transactions, this may be as simple as requesting a photo ID.
- For online and telephone transactions, utilize authenticating procedures. For online authentications, require user logins and passwords or PINS. For telephone transactions, use security questions.
  - Security questions should not be generally available information, such as birthdate, mailing address, or mother's maiden name, that may be easily accessible.

Step #2: Detect Red Flags (cont.)

- Some transactions may not be appropriate to complete via telephone or online and may require in-person authentication. Refer customers to the appropriate process.
- Refuse to complete a transaction if proper identification cannot be provided:
  - For example, a student requests a new BSU ID card, but has no form of picture identification. If you cannot match the identification with information/pictures on file, refuse to issue a new ID until proper identification can be provided.
  - Customer presents a photo ID that does not match his or her appearance. You may need to ask for another form of ID, hold the ID, and possibly contact the Department Red Flags Administrator if appears that someone is impersonating the student or employee.

Step #3: Prevent and Mitigate Identity Theft

Preventing Identity Theft

- Limit access to electronic and paper files containing personal information; only those employees who have a need to access the information should be permitted to.
  - Electronic files should be accessed via a unique user login; employees should not share logins
  - File cabinets and/or offices containing paper records should be kept locked
- Destroy documents or electronic files according to the department's retention schedule when the information is no longer needed. Keep only the information necessary for University purposes.
- Provide clear notice when any form of communication is not secure. For example, email should not be used to transmit Social Security numbers.

Step #3: Prevent and Mitigate Identify Theft (cont.)

Mitigating Identify Theft

- The goal is always to prevent identity theft by using secure systems and following best practices described above; however, if identity theft is discovered reduce the exposure and liability of both the customer and the University by reporting the activity to your **Department Red Flags Administrator**:
  - Report known or suspected fraudulent activity to your department administrator utilizing an **Incident Report Form**
  - Gather all related documentation
  - Provide appropriate contact information
  - Your **Department Red Flags Administrator** will send the report to the University Red Flags Program Administrator

Step #3: Prevent and Mitigate Identity Theft (cont.)

Take immediate action:

- Depending on the nature of the account and/or transaction, your department should have procedures in place to take appropriate immediate action if an activity appears to be fraudulent.
- For example, do you know when and how to:
  - Follow-up to confirm the identity or authorization for unusual activity
  - Cancel or refuse to complete a transaction
  - Notify your Departmental Red Flags Administrator of suspect activity

Step #4: Update and Administer the Program

- While the University and the Red Flags Administrator will update the campus-wide policy and programs, individual departments should work to update and implement processes based on current trends and risks.
- Train your relevant staff; identify employees at many levels who can play a key role in deterrence and detection and make sure they have completed this training as well as training specific to their role.
- Know your environment: which accounts in your department are covered or susceptible to identity theft?
  - Have new accounts been created or old accounts updated? What type of information do they contain?
  - What do identity thieves want and how do they get it?