Where is your institution with Red Flags?

How to catch up fast
Quick Review

• Governed by the Federal Trade Commission
• Applies to any institution, business, organization which extends credit to customers
• Enforcement Deadline delayed until June 1, 2010.
Quick Review

• A pattern, practice, or specific activity that indicates the possible existence of identity theft
• The Rule’s goal is to detect, prevent, and mitigate identity theft in certain 'covered accounts'
• The Rule is actually three different but related rules - all will definitely apply to the following areas:
  – (681.1) Users of Consumer Reports
  – (681.2) Creditors holding ‘Covered Accounts’
  – (681.3) Issuers of Debit and Credit Cards
Higher Education

• Check credit bureau ratings
  – Hiring procedures

• Installment payment plans
  – Student account payments
  – Employee payroll deductions for computer purchases

• Perkins Loan Program

• Branded student cards, i.e. VISA
What is the intent?

• Assumption that identity theft has already occurred
• Pro-active actions that deter or identify the theft in progress
• Assure customer privacy and security
• Increased awareness
Requirements

• Board resolution
• University policy
• Senior management responsibility
• Training program
• Minimal annual review
• Plan of action for reporting and correcting
JMU’s Plan of Action

• Resolution was adopted by BOV in June 2009
• Policy has been approved
• Major areas have been identified
• Training program in the works
• Auto email response to all student or employee address changes or direct deposit changes
Test your knowledge of Red Flags

1. The Red Flag Rules apply to anyone who deals with financing and credit, including car dealerships, banks, physicians' offices, retail merchants, mortgage companies, and cell phone carriers.
   a. True
   b. False
Test your knowledge of Red Flags

• 2. Under the Red Flags Rules, all "covered accounts" must be marked with a small red flag symbol.
  a. True
  b. False
Test your knowledge of Red Flags

- 3. Personal Identification Information (PII) includes:
  a. Any name or number
  b. Any name or number, used alone or in conjunction with any other information
  c. Any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual
  d. None of the above
Test your knowledge of Red Flags

4. "Suspicious" refers to which of the following:
   a. Inconsistent signatures on file
   b. Driver's license photo doesn't match person
   c. Inability to recall mother's maiden name
   d. Phone number given is answered by prison switchboard
   e. Any and all of the above.
Test your knowledge of Red Flags

- 5. Which of the following is **not** a required part of an Identity Theft Prevention Program?
  - a. Reasonable policies and procedures to identify potential "red flags"
  - b. A dedicated phone line for customers to call in identity theft reports
  - c. Specific procedures to detect the "red flags" identified as potential threats
  - d. Appropriate actions to take when "red flags" are detected
  - e. A plan for regularly re-evaluating the program
Test your knowledge of Red Flags

• 6. Red Flags procedures must be "fully implemented" by June 10, 2010. That means:
  a. ...the procedures just have to be written and accessible to everyone
  b. ...the procedures have to be written and everyone needs to be trained to use them
Test your knowledge of Red Flags

7. After you have identified the red flags of ID Theft that you’re likely to come across in your business, what do you do next?

a. Set up procedures to detect those red flags in your day-to-day operations
b. Train all employees who will use the procedures
c. Decide what actions to take when a red flag is detected
d. Periodically review your list of red flags to be sure they are still relevant
e. All of the above
Test your knowledge of Red Flags

8. Because the federal Red Flags Rules are so comprehensive, Virginia's state laws concerning identity theft prevention no longer apply.
   a. True
   b. False
Test your knowledge of Red Flags

• 9. The one thing you will NOT do when you finish this training is:
  a. Identify which of your accounts are "covered" and develop some policies and procedures for how to identify red flags associated with those accounts
  b. Plan training for your employees who will need to be able to detect red flags
  c. Ignore this training and go on with your work - because it's the way things have always been done
  d. Report any known or suspected red flags immediately!
Test your knowledge of Red Flags

10. The purpose of the Red Flags Rules is:
   a. To detect the warning signs – or “red flags” – of identity theft in day-to-day operations, take steps to prevent the crime, and mitigate the damage it inflicts.
   b. To add one more item of busy-work to already overloaded staff, since there's no way to really prevent Identity Theft.