Red Flags Rule

ECU Training Presentation

Provided by the Office of Enterprise Risk Management
Updated 5/13/2013

What is the Red Flags Rule?

- Requires implementation of a written Identity Theft Prevention Program designed to
  - detect the warning signs – "red flags" – of identity theft in day-to-day operations,
  - take steps to prevent the crime, and
  - mitigate the damage it inflicts
- In effect since January 1, 2008 – Enforcement was deferred to December 31, 2010
- Enforced by the Federal Trade Commission (FTC)

How have we responded at ECU?

- The Board of Trustees approved policy "*East Carolina University Identity Theft Prevention Program and Consumer Report Address Discrepancy"* regarding identity theft prevention on April 17, 2009.
- Red Flag Rule program administrator responsibility was given to the Enterprise Risk Management office.
- Additional policies related to Red Flag Rule compliance were subsequently developed in covered account areas (ECUF, Student Health Services, etc.) and a related regulation *"East Carolina University Regulation on Social Security Numbers and Personal Identifying Information"* was also written.
- ECU is also finalizing its new Information Security Standard Manual as well - another part of ECU's Information Security Governance Framework.
- This training was developed and made available to the university community.

Related Definitions

- "Identity theft" – fraud committed or attempted using the identifying information of another person without authority
- "Red flag" – a pattern, practice, or specific activity that indicates the possible existence of identity theft
- "Covered account"
  - An account that the university offers or maintains that involves or is designed to permit multiple payments or transactions for students, faculty, and/or staff
  - Any other account that the university offers or maintains for which there is a reasonably foreseeable risk of identity theft
- "Identifying information" – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person

What is required?

- IDENTIFY – Identify relevant red flags
- DETECT – Detect red flags
- RESPOND – Prevent and mitigate identity theft
- REVIEW – Monitor and update compliance

Indicators to **IDENTIFY** Red Flags

- Notifications and warnings from third-party agencies (e.g. credit agency, law enforcement)
- Suspicious documents (e.g. apparent forgeries, altered documents, physical description or photo does not match person presenting documentation)
- Suspicious identification (e.g. inconsistent statements such as birth dates)
- Unusual use of account (e.g. sudden change in password or mailing address, returned mail, breach in computer security)

How to **DETECT** Red Flags

- Require identifying information before providing access to records online, over the phone, or in person.
- Verify identity of student/ employee in person when possible.
- Verify significant changes in a student/ employee account with the account holder.
- If any of the identifying information appears suspicious you may have detected a red flag.

How to **RESPOND** to Red Flags

- Once detected, take one or more of the following steps depending upon the severity of the breach and department policy:
  - Alert your supervisor and coordinate your response.
  - Continue to monitor the account for evidence of identity theft.
  - Notify the appropriate office of origin for the record/ account.
  - Contact the student, applicant, or employee.
  - Contact the Office of Passphrase Management in ITCS to change any passwords or other security devices that permit/ prohibit access to the account, or report a security incident to the ITCS help desk.
  - Do not open a new account for the student/ employee until the red flag has been cleared.
  - Provide the student/ employee with a new Banner identification number if necessary.
  - In severe instances, notify the East Carolina University Police Department.

How to **RESPOND** to Red Flags
(continued)

- IN ALL CASES notify one of the following officials (and copy Program Administrator – Assistant Vice Chancellor for Enterprise Risk Management):

  - University Registrar – for student account issues
  - University Cashier – for student financial account issues
  - Director of Admissions – for admission issues
  - Director of Financial Aid – for student financial aid issues
  - Associate Vice Chancellor for Information, Technology and Computing Services – for university data issues
  - Associate Vice Chancellor for Human Resources – for employee account issues
  - Your business unit compliance officer or Red Flag Rule program coordinator

REVIEW Your Current Procedures/ Practices

- Secure documents that contain identifying or protected information.
- Ensure that your departmental website, or related portal, is secure through consultation with Information, Technology, and Computing Services.
- Follow university policies for data security.
- Ensure complete and secure destruction of documents and computer files containing account information in accordance with the university's record retention policy and schedules.
- Ensure that all university systems and computers are password protected and virus definitions and protections are up-to-date.

REVIEW Your Current Procedures/ Practices
(continued)

- Sensitive data should not be stored on external drives (USB, Thumb, Flash, etc.).
- Sensitive data stored on portable computing devices and storage media must be encrypted.
- Personally owned drives and devices should never be used to store sensitive institutional data.
- Avoid use of the social security number as an identifier. It is also advisable to avoid using a combination of name, date of birth, address for identification purposes.
- Share this information with employees new to your department and third-party service providers.

The protection of student/ employee information is the job of every employee at

East Carolina University.

These procedures set the minimum requirements for an effective university response.

Departments are encouraged to adopt more specific rules/ procedures/ protections to assist in the implementation of these measures.

The university has several resources available to assist with the protection of university records/ data. If you have a questions concerning these red flag requirements or identity theft prevention in general please contact one of the following university offices:

Office of AVC for Enterprise Risk Management (328-4153)

ITCS Security – Help Desk (328-9866)

Office of the University Attorney (328-6940)

FTC Red Flag Rule Information Also Available at:
http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm

Questions?