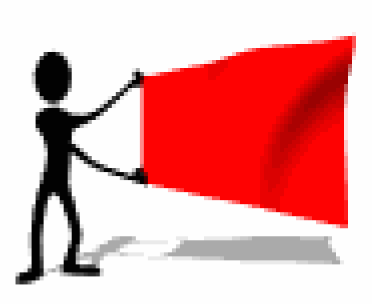

Red Flags Rule

An Introduction

County College of Morris

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

- Enforced by the Federal Trade Commission (FTC)

How have we responded at CCM?

- The Board of Trustees approved policy 2.2018 *"Identity Theft Prevention Program"* on November 17, 2010.

- A document *"Measures for Identity Theft Prevention"* has been developed.

- Training program has been developed and is being made available beginning March 2011.

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 college offers or maintains that involves or is designed to permit multiple payments or transactions for students, faculty, and/or staff

  - Any other account or database that the college offers or maintains for which there is a reasonably foreseeable risk of identity theft to its students, faculty, staff, constituents or customers.

- “Identifying information” – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

- “Service Provider” – a person or business entity that provides a service directly to the College.

What is required?

- IDENTIFY – Identify relevant red flags
- DETECT – Detect red flags
- RESPOND – Prevent and mitigate identity theft
- REPORT – Report attempts of 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 in order to prevent and mitigate identity theft:
  - Alert your supervisor and coordinate a response/notification to the appropriate department of origin for the record/ account.
  - Contact the individual (student, applicant, employee, donor, etc).
  - Change any passwords, security codes or other security devises that permit/prohibit access to the account.
  - Do not open a new account for the individual until the red flag has been cleared.
  - Continue to monitor the account for evidence of identity theft.
  - Determine no response is warranted under the particular circumstance.

How to **RESPOND** to Red Flags

(continued)

– IN ALL CASES notify one of the following officials in writing (and copy Program Administrator – Director of Budget and Compliance):

- Registrar – for student account issues
- Bursar – for student financial account issues
- Director of Admissions – for admission issues
- Director of Financial Aid – for student financial aid issues

How to **RESPOND** to Red Flags

(continued)

– IN ALL CASES notify one of the following officials in writing (and copy Program Administrator – Director of Budget and Compliance):

- Executive Director of Information Systems – for college data issues
- Director of Human Resources – for employee account issues
- Executive Director for Advancement & Planning – for donor related issues
- Vice President for Business & Finance – for vendor and other customer related issues

How to **REPORT** incidents if identity theft

- Manager/director of the office for which the discovery was made shall complete and submit to the Program Administrator the *Identity Theft Detection* form.

REVIEW Your Current Procedures/ Practices

- Secure documents that contain identifying or protected information.
- Avoid the use of social security number as an identifier and limit access to Social Security numbers to employees approved by the Program Administrator.
- Ensure that your departmental website, or related portal, is secure through consultation with the Information Systems Department.
- Follow college policies and procedures for data security.
- Ensure complete and secure destruction of documents and computer files containing account information in accordance with the college's record retention policies and procedures.
- Ensure that all college 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 distributed via email or 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.

- Require and keep only information that is necessary for your business purpose.

- 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

The County College of Morris.

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

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

Questions