University of Arkansas – Fort Smith

Red Flag Training for our
Identity Theft Prevention Program
Red Flag Training Program Adoption

Amendment passed in 2003 to the Fair Credit Reporting Act called “The Fair and Accurate Credit Transactions Act of 2003”

- Required the Federal Trade Commission (FTC), together with other regulatory agencies to issue and enact regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs

- Meant to detect, prevent and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.
Identity Theft Prevention Program

Training is Required

• On an Annual Basis

• As part of UAFS’ Identity Theft Red Flag Training Program

• To help staff detect, prevent and mitigate theft of personally identifiable financial information of UAFS’ customers, as much as reasonably possible
Definitions

Identity Theft

• A 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
Definitions

Covered Account

- Any account designated to permit multiple payments or transactions or one for which there is a foreseeable risk of Identity Theft

Examples include: Student accounts or loans that are administered through the University.

Treat every University account as a covered account.
Definitions

Identifying Information

- Any name or number that may be used alone or in conjunction with any other information to identify a specific person.

Examples include: Name, address, date of birth, social security number, government passport number, student identification number, computer IP address or taxpayer identification number.
Identification of Red Flags

The University identifies the following five Red Flags in the following categories:

- Notification and Warnings from Credit Reporting Agencies
- Suspicious Documents
- Suspicious Personal Identifying Information
- Suspicious Covered Account Activity or Unusual Use of Account
- Alerts from Others
Identification of Red Flags

• **Notifications and Warnings from Credit Reporting Agencies**
  • Report of fraud accompanying a credit report
  • Notice or report from a credit agency or report of a credit freeze on an applicant
  • Notice or report from a credit agency of an active duty alert for an applicant
  • Receipt of a notice of address discrepancy in response to a credit report request
  • Indication from a credit report of activity that is inconsistent with an applicant’s usual pattern or activity
Identification of Red Flags

• **Suspicious Documents**
  • Identification document or card that appears to be forged, altered or inauthentic
  • Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document
  • Other document with information that is not consistent with existing student information
  • Application for service that appears to have been altered or forged
Identification of Red Flags

• **Suspicious Personal Identifying Information**
  - Identifying information presented that is inconsistent with other information the student provides (i.e. inconsistent birth dates or address not matching the address on a loan application)
  - Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
  - Identifying information presented that is consistent with fraudulent activity, such as an invalid phone number or fictitious billing address
Identification of Red Flags

• **Suspicious Personal Identifying Information**
  • Social security number presented that is the same as one given by another student
  • An address or phone number presented that is the same as that of another person
  • A person fails to provide complete personal identifying information on an application when reminded to do so
  • A person’s identifying information is not consistent with the information that is on file for the student
Identification of Red Flags

• **Suspicious Covered Account Activity or Unusual Use of an Account**
  • Change of address for an account followed by a request to change the student’s name
  • Payments stop on an otherwise consistently up-to-date account
  • Account used in a way that is not consistent with prior use
  • Mail sent to the student is repeatedly returned as undeliverable
Identification of Red Flags

• **Suspicious Covered Account Activity or Unusual Use of an Account**
  • Notice to the University that a student is not receiving mail sent by the University
  • Notice to the University that an account has unauthorized activity
  • Breach in the University’s computer system security
  • Unauthorized access to or use of student account information
Identification of Red Flags

• **Alerts from Others**
  • Notice to the University from a student, identity theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft
Detecting Red Flags

- University employees should be on the lookout for possible red flags when dealing with:
  - New Enrollment
  - Existing Accounts
  - Consumer Credit Report Requests
Detecting Red Flags

• **New Enrollment**
  • Verify the following steps to obtain and verify the identity of the person opening the account
    • Require identifying information, such as: Name, Home Address, Date of Birth, Academic Records or Other Identification
    • Verify the Student’s Identity at the time of issuing Student Identification by reviewing Drivers License or Other Government-Issued Photo ID
Detecting Red Flags

• Existing Accounts
  • Monitor transactions on existing accounts:
    • Verify the identity of students if they request information (in person, via telephone, fax or e-mail)
    • Verify the validity of requests to change billing addresses by mail or e-mail and provide the student a reasonable means of promptly reporting incorrect billing address changes
    • Verify changes in banking information given for billing and payment purposes
Detecting Red Flags

• **Consumer Credit Report Requests**
  • Background or Credit Checks (HR only – employment or volunteer positions)
    • Require written verification that the address provided is accurate at the time of the request

• If an address discrepancy is received, verify that the credit report pertains to the applicant for whom the request was made and report to the consumer credit reporting agency an address for the applicant that the University has reasonably confirmed is accurate
Preventing and Mitigating Identity Theft

• **Prevent and Mitigate**
  • Evaluate the risk and take one or more of the following actions

  • Keep all instances of possible identity theft **strictly confidential**

  • Notify **only** your immediate supervisor

  • Continue to monitor the account for evidence of identity theft

  • Contact the student or applicant (for which a credit report was run)
Preventing and Mitigating Identity Theft

• Change any passwords or other security devices that permit access to the account

• Do not open a new account

• Provide the student with a new student identification number

• Supervisors notify a Committee Member to determine if further action is required
Preventing and Mitigating Identity Theft

- **Protect Student Identifying Information**

  - Ensure that all computer files containing identifying information are password protected
  - Log off of your computer when you are away from your desk
  - Make sure that all paper documents are in a secure location and shred identifying information when no longer needed.
    - If you do not have access to a shredding machine, use locked receptacles for disposal of documents
    - Avoid the use of Social Security Numbers whenever possible
    - When necessary to write down a student identification number or social security number, make sure it is shredded or placed in a locked receptacle
Preventing and Mitigating Identity Theft

If you detect any of the identified Red Flags, please take the following steps:

• Notify only your immediate supervisor

• Supervisor should then notify a committee member
Conclusion

• The information that has been presented to you serves only as a guide and is not an all-inclusive list of how identity theft can occur.

• Be aware that identity theft does occur.

• Use caution when setting up new accounts, giving out information on existing accounts, or updating existing accounts.
Reminder . . .

• Annual training is required.

• Please sign and date the *Acknowledgement of Training and Compliance Form*.

• Submit the hard copy of your *Acknowledgement* to the Program Coordinator or Program Administrator.
Committee Members

Mark Horn
UAFS Red Flag Program Administrator
Phone: 788-7035

Helen Seibold
UAFS Red Flag Program Coordinator
Phone: 788-7036