UAFS Identity Theft Prevention Program

Training Outline

A. Define

1. Identity Theft - Fraud committed or attempted using the identifying information of another person without authority
2. Red Flag – Indicates the possibility of identity theft (suspicious activity exists); Due diligence should be performed and noted in detail to protect the University and the student
3. Covered Accounts – Any account designated to permit multiple payments or for which there is a foreseeable risk of identity theft. Treat all University accounts as covered.
4. Valid ID – student ID, driver's license, or other photo ID

B. Watch for Red Flags

1. Notifications & Warnings from Credit Reporting Agencies
2. Suspicious Documents
3. Suspicious Personal Identifying Information
4. Suspicious Account Activity or Unusual Use of Account
5. Alerts from Others

C. Detecting Red Flags

New Student Enrollment: Verify the identity of the person opening an account

1. Require identifying information such as name, home address, date of birth, academic records, or other identification
2. Verify the student's identity at the time of issuing student identification (review driver's license or other government-issued photo ID)

Existing Accounts: Monitor transactions on existing accounts

1. Verify the identity of students if they request information (in person, via telephone, facsimile, or email)
2. Verify the validity of requests to change billing addresses by mail or email (no telephone requests) and provide the student a reasonable means of promptly reporting incorrect billing address changes
3. When a request is made to change information, follow up with an email to confirm the validity of the change.
4. Verify changes in banking information given for billing and payment purposes

Background or Credit Checks (HR only - employment or volunteer positions)

1. Require written verification that the address provided is accurate at the time of request
2. In the event 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 reporting agency an address for the applicant that the University has reasonably confirmed is accurate
D. Preventing and Mitigating Identity Theft

Evaluate the risk and take one or more of the following actions

1. Keep all instances of possible identity theft strictly confidential
2. Notify only your immediate supervisor
3. Your supervisor will then contact a member of the committee
4. Continue to monitor the account for evidence of Identity Theft
5. Contact the student or applicant (for which a credit report was run)
6. Change any passwords or other security devices that permit access to the account
7. Do not open a new account
8. Provide the student with a new student identification number
9. Supervisor is to notify the Program Administrator to determine if further action is required

E. Protect Identifying Information

1. Ensure that all computer files containing identifying information are password protected
2. Log off or lock your computer when you are away from your desk
3. Avoid the use of social security numbers whenever possible
4. When you find it necessary to use a social security number, ask the student to write it down rather than to give it to you verbally
5. Make sure 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)
6. When you find it necessary to write down a student ID number or social security number, make sure it is shredded or placed in a locked receptacle for disposal

NOTE: This outline serves only as a guide and is not an all inclusive list of how identity theft can occur. The important thing is to be aware that identity theft does occur and caution should be used when giving out or updating information.

Committee Members:

- Program Administrator
  - Mark Horn, Interim Vice Chancellor for Finance and Administration
  - Phone: 788-7035

- Program Coordinator
  - Helen Seibold
  - Phone: 788-7036