Red Flags Rule
Identity Theft Training Program

UA LITTLE ROCK

October 2017

Purpose of Training

The purpose of the UA Little Rock Identity Theft Prevention Program is to reduce the exposure of financial and personal loss to both the individual and the university.

Background

- In 2003, U.S. Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACTA).
- Pursuant to this legislation, the Federal Trade Commission issued regulations known as the ***Red Flags Rule***.
- Generally, the *Red Flags Rule* requires financial institutions and creditors that maintain *covered accounts* to develop and implement a written Identity Theft Prevention Program.

Why Must UA Little Rock Comply?

- **The *Red Flags Rule* requires financial institutions and creditors to conduct periodic risk assessment.**
- **UA Little Rock is considered a creditor under FACTA.**
- **While UA Little Rock may not be a financial institution in the typical sense, under the law this determination is based *on whether an organization's business activities fall within the relevant definitions*.**

Annual Training

- **Training is required because**
  - You work in a department that is involved in the creation, modification, or administration of covered accounts.
- **Training will ensure that you are**
  - Knowledgeable and able to take steps to detect, prevent, and mitigate theft of personally identifiable financial information.
  - Able to successfully resolve any identified security risks.
  - Aware of information security.

What is the Difference?

Red Flags

- **The clues you can use to spot possible identity theft. This training will help you identify those clues.**

Identity Theft

- **The actual fraud or theft committed or attempted using the personal identifying information of another person without that person's authority.**

What is a Red Flag?

- **Potential patterns, practices, or activities indicating the possibility of identity theft.**
- **An indication that a fraudulent transaction or event could be occurring as a result of identity theft.**
- **<u>Clues</u> that can be used to spot possible identity theft.**

What is a Covered Account?

- **A covered account is any account that a creditor offers or maintains primarily for personal, family, or household purposes that is designed to permit multiple payments or transactions.**
  - Can be any other account that UA Little Rock offers for which there is a reasonably foreseeable risk of identity theft.
  - Think beyond financial accounts – this may include student files in Admissions or employment applications.

Examples of Covered Accounts

- **Employee payroll deductions**
  - Parking services
  - Recreation memberships and fitness passes
- **Student accounts and financial aid refunds**
- **Installment payment plans**
- **UA Little Rock meal plans and/or Dining Dollars**
- **University loans**
- **Fines or fees from parking or Ottenheimer Library**
- **Background checks or credit reports used for hiring decisions and students enrolled in certain programs**

What is Identifying Information?

- **Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.**
  - Name, address, or telephone number
  - Social Security Number
  - Date of birth
  - Driver's license number, government-issued ID, or student identification number
  - Computer IP address or routing code

Compliance

- **Identify**
  - What constitutes a Red Flag
- **Detect**
  - Red Flags in accounts and operations
- **Respond**
  - Respond to, prevent, and mitigate identity theft
- **Administer**
  - Administer and update the program

Let's Review

Why is UA Little Rock considered a creditor under FACTA?

a. It offers student loans and payment plans for tuition.
b. It issues ID cards.
c. It pays your salary.
d. It is an institution of higher education.

What is a Red Flag?

a. Fraud committed using the personal identifying information of another person without that person's authority.
b. The clues used to spot possible identity theft.
c. Theft attempted using personal identifying information without the person's authority.

Let's Review

Why is UA Little Rock considered a creditor under FACTA?

a. It offers student loans and payment plans for tuition.

b. It issues ID cards.

c. It pays your salary.

d. It is an institution of higher education.

What is a Red Flag?

a. Fraud committed using the personal identifying information of another person without that person's authority.

b. The clues used to spot possible identity theft.

c. Theft attempted using personal identifying information without the person's authority.

IDENTIFICATION OF RED FLAGS

UA LITTLE ROCK

Red Flag Categories

- Notifications or Warnings from Consumer Reporting Agencies
- Suspicious Documents
- Suspicious Personal Identifying Information
- Suspicious Covered Account Activity
- Alerts from Others

Notifications or Warnings from Consumer Reporting Agencies

- **Examples**
  - Fraud alert included with a consumer credit report from a credit bureau.
  - Notice of credit freeze.
  - Notice of address discrepancy.
  - Report or unusual credit activity, such as an increased number of accounts or inquiries.

UA LITTLE ROCK

Suspicious Documents

- **Examples**
  - Documents provided for identification appear to be altered or forged.
  - Photograph on ID does not match the appearance of the individual.
  - Information on the ID does not match the information provided by the person opening the account.
  - Application appears forged, altered, or destroyed and reassembled.
  - Signatures on multiple documents do not match.

UA LITTLE ROCK

Suspicious Personal Identifying Information

- **Examples**
  - The address does not match any address in the consumer report.
  - Correlation between the SSN provided and the range for the date of birth.
  - Duplicate SSN is provided that matches one submitted by another person or another customer with an existing account.
  - Suspicious address is provided, such as a mail drop or prison.
  - When the phone number is invalid or is associated with a pager or answering service.

UA LITTLE ROCK

Suspicious Personal Identifying Information, *continued …*

- **Examples**
  - Duplicate address or phone numbers that match others, or have been supplied by a large number of applicants.
  - The person opening the account is unable to supply identifying information when told the application is incomplete.
  - Applicant's personal information is inconsistent with information already on file.
  - The applicant or existing customer is unable to correctly answer challenge or security questions.

UA LITTLE ROCK

Suspicious Covered Account Activity

- **Examples**
  - Shortly after a change of address on an account, you receive a request for additional users.
  - Drastic change in payment patterns, use of available credit, or spending patterns.
  - An inactive account suddenly has a lot of unusual activity.
  - Mail that has been sent to the customer is repeatedly returned as undeliverable despite continued transactions on the account.
  - You are notified that a customer is not receiving his or her account statements.
  - You are notified of unauthorized charges or transactions on a customer's account.

UA LITTLE ROCK

Alerts from Others

- **Examples**
  - The customer notifies you that he or she has been a victim of identity theft
  - You receive a notification from a third party (such as law enforcement or an attorney) that there is a fraudulent account being used at the university by a person engaged in identity theft.
  - You receive an alert that the security system or procedures have been compromised

UA LITTLE ROCK

Let's Review

Which of the following is considered a covered account and subject to monitoring for Red Flags?

a. Employment applications.
b. UA Little Rock meal plans and/or Dining Dollars.
c. Student accounts and financial aid refunds.
d. All of the above.

A common Red Flag is:

a. Identification documents appear forged.
b. A suspicious address is provided by a student.
c. A photograph on an ID does not match a student's appearance.
d. Personal information is inconsistent with information already on file.
e. All of the above.

Let's Review

Which of the following is considered a covered account and subject to monitoring for Red Flags?

a. Employment applications.
b. UA Little Rock meal plans and/or Dining Dollars.
c. Student accounts and financial aid refunds.
d. All of the above.

A common Red Flag is:

a. Identification documents appear forged.
b. A suspicious address is provided by a student.
c. A photograph on an ID does not match a student's appearance.
d. Personal information is inconsistent with information already on file.
e. All of the above.

DETECT RED FLAGS

UA LITTLE ROCK

Procedures

- **Once you know what a Red Flag looks like, your department must have procedures to detect Red Flags.**
- **Use reasonable procedures to verify the identity of the person you are dealing with.**
  - These procedures may vary depending on the nature of the account and the transaction or information requested.
  - Obtain identifying information about and verify the identity of a person opening/maintaining a covered account.
  - For in-person transactions, this may be as simple as requesting a photo ID.

Authentication

- **Use authenticating procedures for online and telephone transactions.**
  - Online authentications – require user logins and passwords or PINS.
  - Telephone transactions – use security questions.
  - Security questions should not be generally available information, such as birthdate, mailing address, or mother's maiden name.
- **Some transactions may not be appropriate to complete via telephone or online and may require in-person authentication. Refer customers to the appropriate process.**

Proper Identification

- **Refuse to complete a transaction if proper identification cannot be provided.**
  - For example, a student requests a new UA Little Rock ID card, but has no form of picture identification. If you cannot match the identification with information/pictures on file, refuse to issue a new ID until proper identification can be provided.
  - Another instance may be a customer presents a photo ID that does not match his or her appearance. You may need to ask for another form of ID, hold the ID, and contact your immediate supervisor if it appears that someone is impersonating a student or employee.

Consumer (Credit) Report Requests

- **Prior to requesting a background or credit check, obtain written verification from the applicant ensuring that the address and information provided is correct.**
- **If an address discrepancy is found in the completed background or credit check, verify the address with the applicant to ensure the report actually pertains to the applicant for which the report was requested.**
- **Any unresolved address discrepancies should be reported to the consumer reporting agency.**

Service Providers

- The university remains responsible for compliance with the Red Flags Rule even if it outsources operations to a third party service provider.
- The written agreement between the university and the third party service provider requires them to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities.
- Require, by contract, that service providers review UA Little Rock's program and report any Red Flags to the associate vice chancellor for finance.

How to Respond to Red Flags

- **Notify your immediate supervisor.**
- **Immediate supervisor notifies the department head or director to determine any additional steps.**
- **The department head or director notifies the associate vice chancellor for finance.**
- **Continue monitoring activity on the covered account.**
- **Do not contact the accountholder unless directed by the department head, director, or associate vice chancellor for finance.**
- **All instances of possible identity theft must be kept strictly confidential.**

Let's Review

An acceptable document for in-person identity verification is:

a. Birth certificate.
b. Credit or debit card.
c. Photo identification that matches the physical appearance of the person.
d. Social security card.

If you feel there is a possible Red Flag incident, you should:

a. Do nothing.
b. Contact the individual.
c. Notify your immediate supervisor.
d. Talk about the potential identity theft to your co-workers.

Let's Review

An acceptable document for in-person identity verification is:

a. Birth certificate.

b. Credit or debit card.

c. Photo identification that matches the physical appearance of the person.

d. Social security card.

If you feel there is a possible Red Flag incident, you should:

a. Do nothing.

b. Contact the individual.

c. Notify your immediate supervisor.

d. Talk about the potential identity theft to your co-workers.

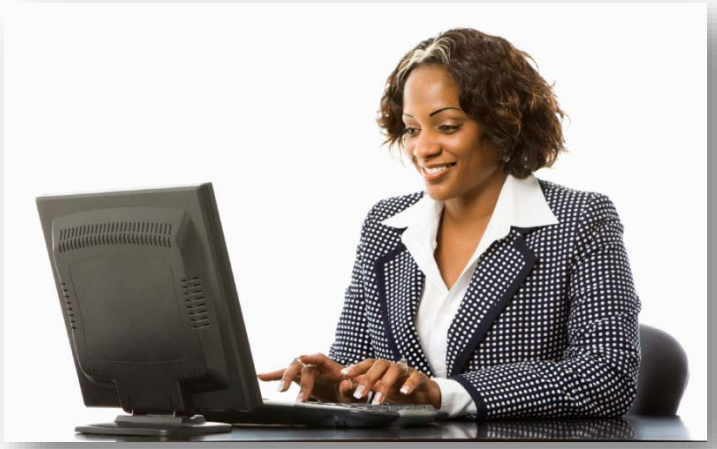
PREVENT IDENTITY THEFT

UA LITTLE ROCK

Internal Operating Procedures

UA Little Rock incorporates these internal operating procedures to protect student identifying information.

- Any university website that is used to access student accounts is secure or provides clear notice to all users that the website is not secure.
- Departmentally controlled IT resources (network, servers, applications, individual workstations, etc.) are maintained in strict compliance with UA Little Rock's Information Security Program best practices.



Internal Operating Procedures

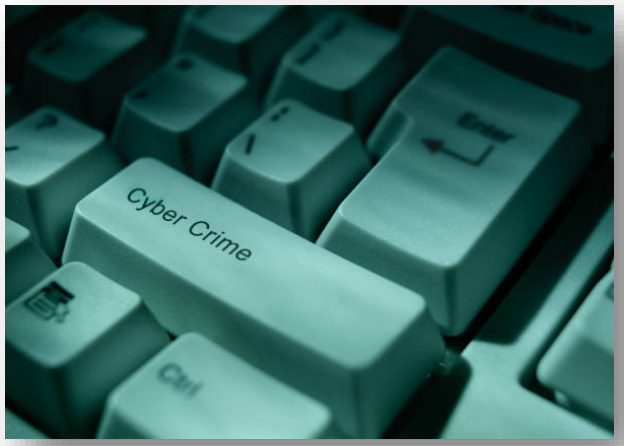
UA Little Rock incorporates these internal operating procedures to protect student identifying information.

- Employees keep sensitive documents and working materials out of the public view while working.
- Sensitive documents and working materials are secured during breaks and non-working hours.
- File cabinets that contain sensitive or confidential documents are located in a secure area.
- Employees are trained or otherwise required to use shredders for sensitive or confidential documents.

Internal Operating Procedures

UA Little Rock incorporates these internal operating procedures to protect student identifying information.

- Computer files containing sensitive or confidential information are stored in a secured manner.
- There are adequate procedures in place to ensure that only necessary access to information system resources are made available to employees to perform their job (principle of least privilege).



UA LITTLE ROCK

Internal Operating Procedures

UA Little Rock incorporates these internal operating procedures to protect student identifying information.

- **All office computers which store or access student account information are password protected and follow all other computer security best practices as established by UA Little Rock's information security program.**
  - Employees are required to use a strong password for access to their computer and other systems.
  - If employees are allowed to work remotely, secure methods are used to access IT resources and transmit files (e.g., the use of VPN, security of laptops, encryption, etc.).
  - Employees are required to lock their computers and/or use password protected screen savers when they leave their work area.

UA LITTLE ROCK

EXAMPLE OF A RED FLAG INCIDENT

UA LITTLE ROCK

Example

Jane works in the Bursar's Office. She receives a call one day from a student requesting information on a refund check that should have been mailed to her weeks ago. Jane, according to Bursar's procedures, asks the student to verify her birth date and asks her what courses she is taking the current semester. The student provides information that matches the system data.

Jane determines that a refund check was issued two weeks ago. She looks up the mailing address and asks the student to verify this address. The two addresses do not match. The address the student provides was "inactivated" when a new address was entered. Upon further investigation, the address was not changed online by the student but by another department.

Jane sees a Red Flag. She informs the student she will look into the matter further and someone will call her back. Jane immediately reports the Red Flag to her supervisor. Her supervisor looks into the matter and finds that the check was cashed but the signature on the copy of the cancelled check does not match any other signatures on prior checks or other documentation signed by the student.

Example

Jane's supervisor determines that this is definitely a possible identity theft situation. She contacts the associate vice chancellor for finance, prepares a written report, and contacts the Department of Public Safety. The Department of Public Safety will contact the potential identity theft victim (student) and investigate fully.

This incident and any others that occur will be included on the annual report submitted by the associate vice chancellor for finance to the UA Systems Office.

Further information:

- The department that changed the address should have asked for other documentation showing the new address and a photo ID as verification of the identity of the individual and evidence of a valid address. Or, the student should have been directed to change the address online with a logon ID and password.

- Because the signature is not hers, an affidavit must be completed and submitted to the bank. The student may be issued another check upon completion of a full investigation by the bank, the Department of Public Safety, and/or any other applicable law enforcement agency.

Let's Review

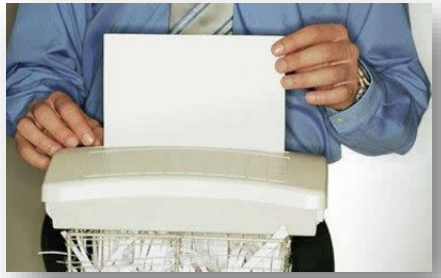
To prevent identity theft, employees must:

a. Use shredders for sensitive or confidential documents.

b. Securely store computer files that contain confidential information.

c. Lock computers and/or use password protected screen savers when leaving the work area.

d. All of the above.



Let's Review

To prevent identity theft, employees must:

a. Use shredders for sensitive or confidential documents.

b. Securely store computer files that contain confidential information.

c. Lock computers and/or use password protected screen savers when leaving the work area.

d. All of the above.

FINAL MATTERS

UA LITTLE ROCK

Audit Requirements

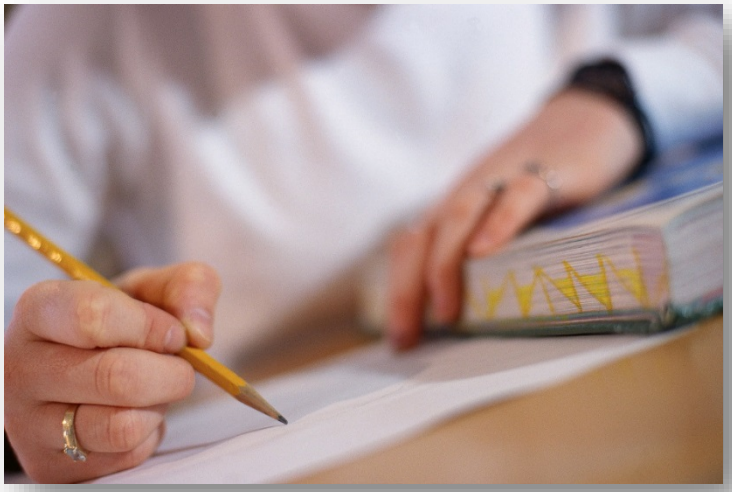
Each department should perform periodic audits to ensure that unauthorized individuals do not have access to personal identifying information or files and are not accessing them.

Oversight

- **The Identity Theft Committee is responsible for developing, implementing, and updating the program. Committee members include representatives from all tested departments.**
- **The committee is chaired by UA Little Rock's associate vice chancellor for finance, who also serves as the Program Administrator.**
  - Ensures program is periodically reviewed.
  - Ensures that training is completed annually.

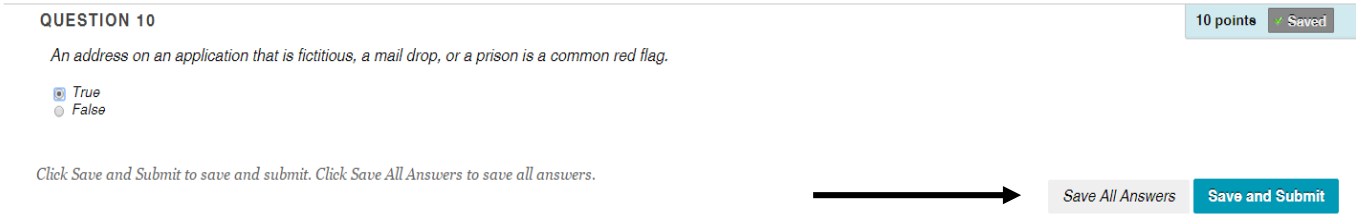
Assessment

- Click in the training program link in the menu to the left.
- Click the Assessment link.
- Complete the Assessment with a minimum score of 80%.
- Repeat as many times as necessary.
- Refer back to training presentation and materials at any time if needed.

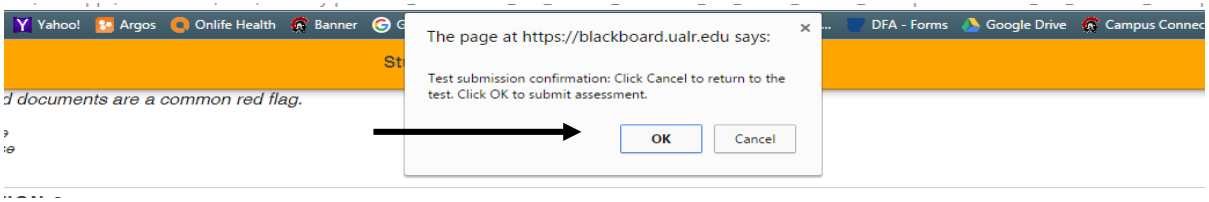


View Assessment Score

1. **After completing the assessment, click Save and Submit:**

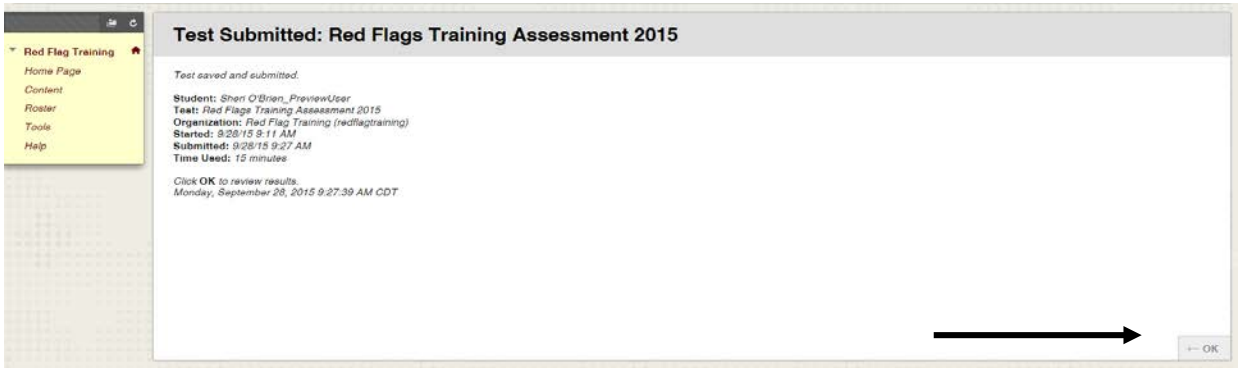


2. **Click OK in the pop up screen – "Test Submission Confirmation."**

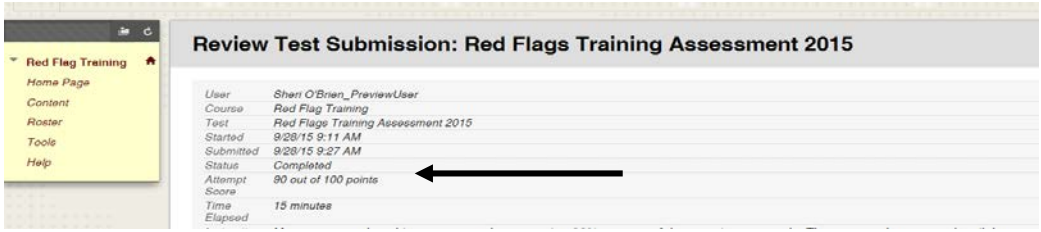


View Assessment Score

3. **Click OK in the bottom right of the screen to view results.**

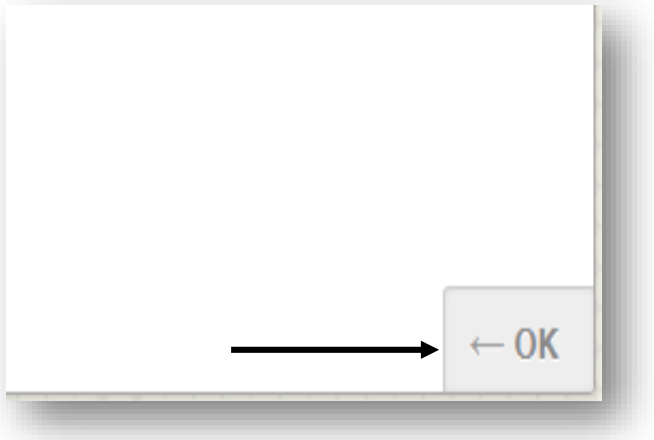


4. **Attempt score will be in the header.**



View Assessment Score

- A review of each question with feedback on correct and incorrect responses will display below the header.
- Re-take the assessment if your score is below 80%.
- Exit by clicking OK in the bottom right corner.



Program Evaluation

Finally, please evaluate this training program by clicking the training program link in the main menu and then the Evaluation link. Responses are strictly anonymous and will assist us to refine and improve future training programs.

Thank You For Your Participation

Red Flags Rule Identity Theft Training

University of Arkansas at Little Rock
October 2017

Other source materials:

UA Little Rock Identity Theft Prevention Program
Federal Trade Commission Red Flags Rule
Ball State University's Identity Theft Protection Program
California State University Red Flag Identity Theft Training