
UTEP
OFFICE OF
INSTITUTIONAL COMPLIANCE
Red Flags Rule – Detecting, Preventing, and Mitigating Identity Theft

What is Covered?

- The Red Flags Rule
- Entities who must be in compliance
- UTEP Departments and Offices responsible for Opening or Maintaining covered accounts
- Personal Identifying Information
- Four Steps to Compliance
- Scenario of Red Flags Rule
- **Teachable Takeaways**
- Additional Resources

The Red Flags Rule

- The **Red Flags Rule** is a U.S. federal regulation designed to help **prevent identity theft**. It requires certain businesses and organizations to **develop and implement written identity theft prevention programs**.
  - An Identity Theft Prevention, Detection, and Mitigation Program must be developed, implemented, and administered.
  - These rules have been in effect since January 1, 2008.
  - Applies to **"financial institutions"** and **"creditors"** that offer or maintain **covered accounts**.

Red Flag definition

- A **red flag** is a **warning sign or pattern** that indicates the **possible risk of identity theft.**
- **Examples Include:**
  - Suspicious account activity (e.g. changes in spending patterns)
  - Alerts from credit reporting agencies
  - Inconsistent or suspicious personal information
  - Lost or stolen ID documents
  - Mail returned undelivered despite an active account

Entities who must Comply

- Financial Institutions
- Creditors such as: Utility Companies, Healthcare Providers, Auto Dealers, Mortgage Brokers.
- Universities and colleges that provide installment payment plans, student loans, or process student loan applications – these universities and colleges are considered creditors.
- **The definition further describes "covered accounts," which are accounts where there is a foreseeable risk of identity theft, and the account can be accessed remotely through the Internet or cell phone.**

UTEP departments and offices responsible for opening or maintaining covered accounts

- Athletics Department
- Enrollment Services
- Extended University
- Graduate School
- Human Resources
- Information Security Office
- Technology Support
- International Programs
- Military Services
- Miner Gold Card Office
- Office of Scholarships
- Office of Undergraduate Admissions & Recruitment
- Parking & Transportation
- Professional and Public Programs
- Registration & Records
- Student Business Services
- Office of Student Financial Aid
- Study Abroad
- University Police

Personal identifying information

- Information that may be used alone or with other information to identify an individual, includes, but is not limited to:
  - Name
  - Social Security Number
  - Date of birth
  - Telephone/cell number
  - Government issued driver's license or identification number
  - Alien registration number
  - Passport number
  - Employer or taxpayer identification number
  - Credit/debit/banking account numbers

Four steps to compliance

- Step 1: Identifying Red Flags
- Step 2: Detecting Red Flags
- Step 3: Preventing and Mitigating Identity Theft
- Step 4: Updating UTEP's program

Step 1: Identifying Red Flags

- There are **5 common Red Flags of Identity Theft that you should be on the lookout for**:
  - Category 1: False alerts, notifications, and warnings from credit reporting agencies
  - Category 2: Suspicious documents
  - Category 3: Suspicious personal identifying information
  - Category 4: Suspicious account activity
  - Category 5: Notices from other sources

Category 1: False alerts, notifications and warning from credit reporting agencies

- Most university departments do not request credit reports on a regular basis. However, if your department does use credit reports, red flags may include:
  - Report of fraud accompanying a credit report
  - Notice from a credit agency of a credit freeze
  - Notice from a credit agency of an “active-duty alert”
  - Receipt of address discrepancy in response to a credit report request
  - Indication from a credit report of activity inconsistent with an applicant’s usual pattern or activity

Category 2: Suspicious documents

- Suspicious documents include employment applications, applications for admissions, taxation and revenue documentation, and change of address requests. Red flags may include:
  - Identification documents or cards that appears to be forged, altered, or inauthentic
  - Identification documents or cards in which a person's photograph or physical description is not consistent with the person presenting the document
  - Other documents with information that is not consistent with existing student/employee information
  - Applications that appear to have been altered or forged

Category 3: Suspicious personal identifying information

- When assisting the UTEP community, properly identifying information is needed – this may include a student ID, driver's license, or passport.
- Over the phone, employees should verify the date of birth or other personal information. Red flags may include:
  - Inconsistent identifying information, such as inconsistent date of birth
  - SSN that has not been issued or is listed on the Social Security Administration's Death Master File
  - Failure to provide complete personal identifying information on an application when reminded to do so
  - Identifying information presented that is consistent with fraudulent activity, such as an invalid phone number or fictitious billing address

Category 4: Suspicious account activity or unusual use of account

- Any of the following should be considered a Red Flag:
  - Change of address on account followed by a request to change the student's name
  - Payments stop on an otherwise up-to-date account
  - Mail sent to a student is repeatedly undeliverable although there is account activity
  - Notice to UTEP that the student is not receiving any university mail
  - Notice to UTEP that the account has unauthorized activity
  - Unauthorized access to or use of student account information
  - A breach in UTEP's computer system security

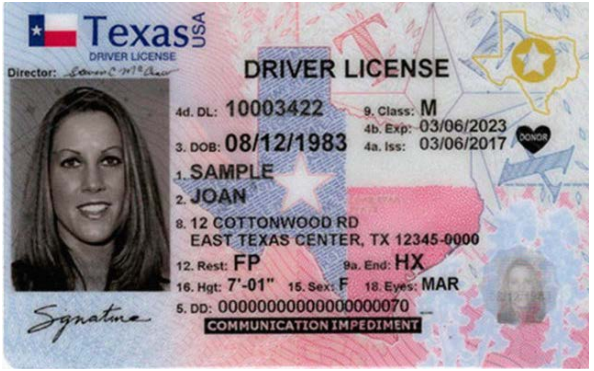
Category 5: Notices from other sources

- An obvious Red Flag occurs whenever notice is given to the University from:
  - A student
  - An identity theft victim
  - Law enforcement authorities

Unmistakable signs of false identification

- Quality of print is poor or indistinct
- Holograms or ghost images do not appear in high quality
- Magnetic strip is covered by plastic laminate
- State seal or camera number is partially covered by photo or has been altered
- Lettering does not match or appears altered
- ID is expired
- Numbers have been scratched, bleached out and inked over, or cut out and reinserted
- Picture does not resemble bearer
- Bearer cannot quickly state date of birth or address
- Bearer’s signature does not match signature on identification
- Driver’s license does not match a legitimate sample (compare it to the one in your own wallet!)
- Lamination seems too thick or has cuts or overlays
- Lamination has air bubbles, peeled back corners, or faulty re-sealing

Newly redesigned Texas Drivers License and ID cards



- New Texas Drivers License Security features:
  - Laser engraving and polycarbonate card body
  - Heart shaped Organ Donor identifier
  - Texas Real ID-compliant card is marked with a gold star on the upper right hand corner
  - Raised tactile text represents ID number and issuant' s name
  - Under 21 indicator identifies when issuant is a minor
  - Communication Impediment Identifier available to indicate a health condition that may impede issuant' s ability to communicate
  - Identifiers on the front of the license or ID identifies health conditions and Veterans/Disabled Veterans service
- Source: Texas Department of Public Safety newly redesigned Texas DL and ID Cards brochure, 2021 **https://www.dps.texas.gov/sites/default/files/documents/driverlicense/documents/newdlidcards.pdf.**

Mid-module questions

Question #1 (Refer to Slide #3)

The Red Flags Rule applies to universities and colleges that provide installment payment plans, student loans, or process student loan applications and are considered creditors.

True or False

Question #2 (Refer to Slide #3)

Which UTEP department(s) are responsible for opening or maintaining “covered accounts”?

a. Student Business Services
b. Registration and Records
c. Human Resources
d. Miner Gold Card Office
e. All of the Above

Step 2: Detecting Red Flags

- Areas of particular concern are:
  - Obtaining identifying information about and verifying the identity of a person opening/maintaining a covered account. This is as simple as requesting a picture ID anytime a student conducts business with your department.
    - In the case of issuing a Miner Gold Card to a new or existing student, staff must request additional photo identification and verify information such as address and date of birth.
  - Authenticating customers, monitoring transactions, and verifying the validity of change of address requests.
    - For example, Student Business Services authenticates identity by requiring a student to present an ID in person and by verifying class schedules over the phone. This office will not change account addresses and will refer students to complete a change of address online.

Step 3: Preventing and Mitigating Identity Theft

- In the event UTEP personnel detect any identified red flags, these individuals should discuss the situation with their supervisors who will take one or more of the following steps, depending on the degree of risk posed by the Red Flag. Prevention and mitigation may include:
  - Continuing to monitor an account for evidence of identity theft
  - Contacting the student or applicant
  - Changing passwords or other security devices that permit access to the account
  - Not opening a new account/admit student
  - Providing the student with a new ID number
  - Notifying the department Dean or Director
  - Notifying the Program Administrator for determination of the appropriate steps to take
  - Notifying law enforcement
  - Determining that no response is warranted under the particular circumstances

- Protect student/employee identification by:
  - Ensuring that the **utep.edu** website is secure (or provide clear notice that the website is not secure)
  - Ensuring complete destruction of paper documents and computer files containing student account information when no longer needed
  - Ensuring that office computers with access to account information are password protected
  - Avoiding use of Social Security Numbers
  - Ensuring computer virus protection is up-to-date
  - Requiring and keeping student information that is only necessary for University purposes

Step 4: Updating UTEP's Program

- UTEP's Handbook of Operating Procedures (HOP) Section VII: Financial Services, Chapter 8.4.2.2, includes the following:
  - The sub-program will be reviewed as scheduled by the Associate Vice President of Business Affairs, but no less than annually, and will be revised to reflect changes in operations and changes in potential risks of identity theft.
  - UTEP employees with responsibility under the Annual Program will receive initial training and periodic training as necessary to ensure compliance with the Identity Theft Prevention, Detection and Mitigation Program.

Scenario: Red Flags Rule

Category 4: Suspicious account activity or unusual use of account

- **Example**: A student visits Student Business Services (SBS) to report that his direct deposit information was updated without his consent.
  - SBS staff member authenticates identity by requiring the student to verify his student ID number and provide a valid identification.
  - SBS staff member directs the student to reset his UTEP password, update his direct deposit information accordingly and report the issue to the **Information Security Office (ISO)**.
  - SBS staff member determines that the student has a credit on his account.
    - SBS staff member informs the student that a paper check will be issued for pick-up instead of direct deposit.
    - SBS staff member immediately reports the Red Flag to their supervisor.
    - After confirming there is an issue, the supervisor reports the issue to the **ISO**, **Accounts Payable** and **IT** for further investigation/action.
    - After further investigation, it is discovered that the student's UTEP credentials were compromised after clicking on a hyperlink in a recent phishing email.
    - This incident, and any others that occur, will be included on the periodic report submitted to **The Office of the Vice President for Business Affairs (VPBA)**.
- **Corrective Action:**
  - The student was informed he should not have provided his UTEP credentials by clicking on the hyperlink provided to him on the phishing email.
    - The student was informed that his UTEP credentials should only be entered directly onto the **UTEP Single Sign On**.
  - The student was issued a paper check refund for pick-up after affirming that he reset his UTEP password and updated his direct deposit information.

Teachable Takeaways

- UTEP employees should be on the lookout for five (5) common Red Flags of Identity Theft:
    1. False alerts, notifications, and warnings from credit reporting agencies
    2. Suspicious documents
    3. Suspicious personal identifying information
    4. Suspicious account activity
    5. Notices from other sources

- It is vital that UTEP employees understand how to spot:
    - Fraudulent personal identification, and
    - Bearer's lack of information when asked, as caution.

- In the event of detecting a red flag account, it is the responsibility of UTEP employees to direct their findings to their supervisor and follow procedure to then mitigate the threat to protect the student/employee affected.

- Red flag rules are designed to detect, prevent, and mitigate any warning signs of threat, in day-to-day operations.

Additional resources

- **Federal Trade Commission (FTC)**
  https://www.consumer.ftc.gov/features/feature-0014-identity-theft

  https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule

  https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf

- **HOP Section VII Financial Services, Chapter 8: Identity Theft Prevention, Detection and Mitigation Policy (Red Flags Rule)**
  https://www.utep.edu/hoop/section-7/ch-8.html

- **For additional information or to report incidents of identity theft, please contact:**

  Office of the Vice President for Business Affairs (VPBA)
  Administration Building, Ste. 301
  El Paso, Texas 79968
  Telephone: (915) 747-5113
  Fax: (915) 747-5068

End-module questions

Question #1 (Refer to Slide #11)

Student Business Services can verify a student's identification with a valid ID and by verifying their class schedule.

True or False

Question #2 (Refer to Slide #14)

A student visits Student Business Services (SBS) to report that his direct deposit information was updated without his consent. The student can request a paper check if they are due a refund.

True or False

Question #3 (Refer to Slide #16)

To report incidents of identity theft, students can contact:

a. Vice President of Student Affairs
b. UTEP Police Department
c. Vice President of Business Affairs
d. Financial Aid