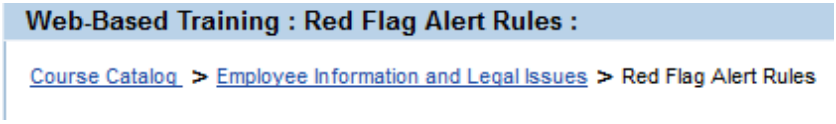
Texas State University

Office of Procurement and Strategic Sourcing
512.245.2521 | purchasing@txstate.edu

Red Flag Fraud Alert Reminders

Access this training via: https://www.txstate.edu/sap/



What is a red flag?

A pattern, practice, or specific activity that indicates the possible existence of fraud.
It can be something someone says, or does, or something that happens on an account that is unusual or suspicious. Texas State uses various sources to verify the identity of our vendors.

Look out for:

- Alerts or notifications from a consumer reporting agency.
- Phishing- These emails attempt to get you to open a document or link that may harm your computer or expose personal information.
- Suspicious documents:
    - Documents that appear to be altered, forged or information that does not agree with data already on file.
- Suspicious personal identifying information
    - The person attempting to update or open a new account fails to provide all personally identifying information.
- Unusual use of, or suspicious activity related to a covered account
- Notification that the account is being used for identity theft.

What to do if you suspect fraud:

- Notify your supervisor.
- Send suspected phishing attempts to: abuse@txstate.edu
- Investigate to the extent needed to determine if identity theft is likely or a data breach has occurred.
- Assess whether a response is needed and take immediate action if necessary.
- Notify your Identity Theft Prevention Program Administrator, Internal Audit, and UPD to plan your response.

Actions to Consider:

- Cancel the suspected fraudulent transaction if possible.
- Contact abuse@txstate.edu
- Change any passwords or security codes that permit access to the account.
- Monitor activity on the account.
- Place a hold on the account.
- Close the account.
- Reopen the account with a new account number.
- Refuse to open a new account.