Vendor Setup Procedures Security Summary

Submitting Vendor Setup Applications

- Non-employee Vendors Complete and fax 1) Vendor Coversheet, 2) W-9, 3) Direct Deposit Form to AP Vendor ID @ (713) 743-0521.

- Employee vendors complete and fax 1) Vendor Coversheet and 2) W-9 to AP Vendor ID @ (713) 743-0521. Employee vendors will then enter their ACH bank account information via P.A.S.S.

- **All vendor setup forms must be submitted directly from vendors via fax.** The following vendor setup applications will NOT be accepted:
    - Forms sent via e-mail
    - Forms sent from university departments

  Why: Requiring items to come direct from the vendor and only by fax provides both the Vendor and the System with additional and necessary assurance that the information received is accurate and secure. These are additional internal controls that we are implementing after discussion with Internal Audit and our executive leadership.

- *This process will be automated when the Vendor Management System is implemented. Departments can send invites to vendors via the system, and the vendors will submit the vendor application via the system.*

Verification of Vendor Setup Applications

- **AP Vendor ID reviews all new Vendor Requests and Change Requests for "red flags"**
- Red Flags include
    - Frequent banking changes
    - TIN that does not agree across forms
    - TIN and Banking information that does not agree to information on file
    - Unusual qualities to the request, such as email addresses that do not contain the company name, unusual dating formats, fax stamps that do not agree to the company, missing fax stamps
- Red Flag items require AP Vendor ID to do independent confirmation of the accuracy and veracity of the submitted set up or change request

- **AP Vendor ID confirms certain changes directly with the Vendor:**
  All changes to direct deposit, address, contact name, and phone number and e-mail will be verified with the vendors. AP Vendor ID will contact the vendor and verify the changes.

- *The verification process will be automated when the Vendor Management System is implemented.*

What Can Departments Do To Help

- Tell Vendors that they must send their documents directly to AP via fax. This is to protect the University, its employees, and its business partners and vendors.
    - We are working with IT to help ensure that fax processes work better
- Know what the most frequent attacks are in Purchasing and Accounts Payable:
    - Payment fraud – getting banking or address information changed for a real vendor in order to divert payments
    - Ordering fraud – sending other companies fraudulent purchase orders from the university in order to obtain merchandise
- Know that most fraudsters rely on social engineering – they rely on convincing someone on the inside to unwittingly help them get someone else to break normal security procedures.
- Vendors may still request assistance and information from campus departments. Because fraudsters often rely on an "insider", some of the things that AP looks for that may be helpful to departments in detecting dishonesty are:
    - Emails may appear to be from the vendor, but out of the ordinary requests, especially those that ask for information or assistance in getting information changed include:
        - Comes from an email address that does not include the business name
        - Comes from an email address that is similar to that of the vendor but is off just a little. For example, spoofs of UH email addresses will use "uh-edu.com" or "uh.edu.us"
        - Uses a website that is similar to that of the vendor but is off just a little
        - Is poorly written, with misspellings and awkward sentence structure
        - Contain addresses and contact phone numbers that do not make sense (ex: Texas companies with foreign phone numbers)
    - Emails for information or requests for assistance them with getting set up that reference executives that do not make sense to be involved for the situation.
    - Invoices and demands for payment for items you did not order or receive
    - Unusual requests, such as asking you to give them a list of all of their past payments because they have had "a banking error" and don't know if they were paid
    - Requests to help them get information that the vendor should have (their bank account, their TIN, their address)
    - Requests for assistance in getting another area to override their business processes because it's an emergency
    - Insistence that something must be accomplished immediately or outside of the standard business practice even after you have explained the business process to them
    - Threatening or angry responses to requests for additional information or that business processes be followed