Vendor Setup Procedures Security Summary

Submitting Vendor Setup Applications

This is an automated process through PaymentWorks. Departments can send invites to vendors via the system, and the vendors will submit the vendor application via the system.

To ensure no duplicate invitations are sent to vendors, see the steps to follow before sending an invitation at "Initiator Role (Review for Duplicated Registration and Invitation)" in the PaymentWorks section of the AP-General website at https://uh.edu/office-of-finance/ap-general/.

Verification of Vendor Setup Applications

- **PaymentWorks and AP Vendor ID reviews all new Vendor Requests and Change Requests for "red flags"**
- Red Flags include
    - TIN that does not agree with the business or legal name per IRS records.
    - W-9 or W-8 documentation that does not agree with the name and TIN provided within PaymentWorks
    - Frequent banking changes
    - Tax or business information that does not agree across documentation
    - 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
- Red Flag items require PaymentWorks and/or AP Vendor ID to do independent confirmation of the accuracy and veracity of the submitted set up or change request

- **PaymentWorks confirms certain changes automatically or directly with the Vendor:**
    - All banking information. PaymentWorks will either automatically validate or will contact the vendor and verify the changes.
    - TIN vs. Legal Name. PaymentWorks will automatically validate per IRS records.

What Can Departments Do To Help

- Invite in PaymentWorks only those vendors that you currently plan to utilize.
- Do not fill out documentation in PaymentWorks on behalf of a vendor.
- Do not advise a vendor on how to complete their tax documentation. While vendors struggle to complete their W-9 or W-8, UH cannot advise them on personal or business tax matters.
- Tell Vendors that they must send their documents directly via PaymentWorks. This is to protect the University, its employees, and its business partners and vendors.
- Advise the vendor to use the Vendor Setup and Update Guide online at https://uh.edu/office-of-finance/vendor/vendor-setup-and-update-guide/.
- 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 are out of the ordinary requests, especially those that ask for information or assistance in getting information changed, including:
        - 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 with getting set up that reference UH 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