Purchase Order Fraud Notice

Please be on high alert for emails requesting quotations or purchase orders that purport to originate from the University of Texas System Administration (UT) but are in fact fraudulent. While UT cannot prevent this illegal activity, we are actively working with law enforcement to investigate these fraudulent emails.

There are several ways to determine if a PO is fraudulent. It all starts with attention to detail. There are several red flags that should go up when examining a questionable purchase order.

- **Look** at the sender's email address. Are there subtle differences in the domain, like dashes instead of periods? (i.e. Joe.Smith@StateAgency-State.us rather than Joe.Smith@StateAgency.State.us)
- **Examine** the sender's name. Is their name unfamiliar or does their name match up with the partner contact on-file? If there was a changing of procurement personnel with a partner, is there an email documenting this?
- **Check** the phone numbers in the email. Are they also associated with the partner on-file? Maybe the local phone number is correct, but the area code is off.
- Critique the grammar. Scammers are constantly sending emails to numerous targets and they don't always take the time to ensure their emails have proper spelling or sentence structure.
- The message requests shipment/delivery of products to non-University of Texas addresses.
- The message may include an attachment that is designed to look like a purchase order, may include a logo or other graphic, and a signature that may look legitimate. UT does not publish solicitations with handwritten signatures.
- Consider the quantity/quality of items. Does either the quantity or type(s) of the good(s) requested seem in excess? If it appears unusually high for either one, proceed with caution.
- There's a demand for rush delivery. If the PO stresses a sense of urgency that an order must be sent using priority or over-night mail, there may be reason for concern.
- The PO you receive lists a legitimate UT shipping address, but you later receive a request to modify that shipping address to a non-UT address. This is a common practice of scammers to reroute shipments to a desired delivery point.

If you believe you have received a fraudulent email that appears to be from UT System Administration, please forward it to UT System Purchasing for review.