

Notice to Suppliers – Fraudulent Purchase Order Activity via Email or Other Means

The WVU Department of Procurement, Contracting and Payments Services wants to alert suppliers to an email scam that involves requests for quotes, establishment of credit, or submission of a purchase order, which appears to originate from WVU, but is in fact fraudulent.

While WVU cannot prevent this illegal activity, we are actively working with law enforcement to investigate fraudulent email contacts and to address fraudulent purchase orders issued in WVU's name as we become aware of them.

Although this investigation is ongoing, we can share with you some common traits or themes of these fraudulent emails which may help reduce the risk to your company.

- The email message is poorly written with misspellings and awkward sentence structure
- The sender's email address or website link are not the same as WVU's standard @mail.wvu.edu email address domain
- The delivery zip code listed in the email is something other than WVU's 26506 zip code
- The message requests shipment/delivery of products to a non-WVU address
- The quote requests large quantities of highly resalable items

Examples of fraudulent email address domains that have been used are:

- @mail-wvuedu.com
- @aol.com
- @wvu-edu.org

The message may include an attachment designed to look like an official request for quote or purchase order, an email signature appearing to represent a WVU employee, an authentic logo or WVU watermark copied from our website, or contain some other graphic designed to look legitimate.

If you are not familiar with the documents provided and/or content of a WVU purchase order or suspect fraud, please contact us immediately before responding or filling the order.

WVU and its Procurement Department value our partnership and appreciate the important role you play in providing goods and services to WVU faculty, students, and staff.

Respectfully,

WVU Purchasing, Contracts and Payment Services