Dear Campus Community Member,

There has been a recent issue with fraudulent requests for quotes and purchase orders purportedly from the University of Oregon being distributed to our vendor communities. The false emails are generated from a uoregonregents.com address and have a false signature block for Catherine Susman or Daniel Patten.

If you receive any emails or requests for quotes or purchase orders that you are suspicious of, please immediately send them to contract@uoregon.edu.
Purchase Order Scams

PURCHASE ORDER SCAMS TARGETING U.S. COMPANIES AND UNIVERSITIES

Purchase order scams (often originating from entities in Nigeria) routinely use legitimate business and university identities to fraudulently obtain merchandise from vendors. More than 445 attempted incidents have been tracked by the FBI, with over 90 companies and universities targeted since late 2010. The vendors, businesses, and universities are typically unaware of the scam until after the merchandise has been exported out of the country. The merchandise consists of items that can be easily resold, such as computers, projectors, cameras and pharmaceutical and industrial equipment. The scams, typically conducted through online and telephone social engineering techniques, make retailers believe they are filling a request for an established customer.

Upon suspicion of a scam, companies should immediately contact their local FBI Field Office, which will allow for a greater chance for the items to be located and returned. Companies may also submit suspicious online activity via the Internet Crime Complaint Center website (www.ic3.gov), which will provide reports directly to both the FBI and the National White Collar Crime Center (NW3C).

The purpose of this SPIN is to inform U.S. companies, universities, and vendors of a prevalent scam intended to defraud establishments out of millions of dollars.

TECHNIQUES USED WITH PURCHASE ORDER SCAMS

The scam has several variations, however, it essentially follows this course of action:

Step 1: Criminal establishes domain names similar to a well-known business/university.
Step 2: Establish phone numbers falsely associated with the impersonated entity.
Step 3: Establish U.S. addresses to receive and re-ship products.
   - Use dating sites or work from home ads to acquire U.S. address.
   - May often use a self-storage or warehouse address.
Step 4: Request product quotes using email accounts on bogus domains.
   - Often requests estimates for larger amounts/quantities.
Step 5: Email purchase orders on fabricated letterhead.
Step 6: Obtain tracking information from the victim company to determine if/when the packages will be delivered.
Step 7: Arrange reshipment, generally sending shipping labels to the re-shipper.
   - Merchandise is shipped to Nigeria, often through the United Kingdom, or directly through freight forwarders.
Step 8: Victim vendor bills the university or company being impersonated.
   - Vendor does not learn of the fraud until the real company or university receives the invoice and notifies the vendor.

INDICATORS OF FRAUD

- Incorrect domain name on email and post office boxes.
- Shipping address is not the same as the business location.
- Delivery address is a residence or self-storage facility.
- Poorly written email with grammatical errors.
- Phone numbers not associated with the company/university.
- Unusually large quantities are requested.
- Rush to ship priority/overnight.

The product was prepared by the FBI Strategic Partnership Unit. If you have any information regarding purchase order or similar scams, or have questions or comments, please contact your local FBI Office or FBI Strategic Partnership Coordinator.