



## **Notice to Suppliers – Fraudulent Quote & Purchase Order Activity via Email**

**\*\*\*Genuine emails from UNM always end in **".edu"** (not .com, .net, etc)**

We want to alert you to an active email scam involving purchase orders and request for product quotations that purport to originate from the University of New Mexico, but are in fact fraudulent. While the University cannot prevent this illegal activity, we are actively working with law enforcement to investigate these fraudulent email contacts. This type of scam has hit many colleges and universities in the past few years.

Here are some common traits or themes of these fraudulent emails that may help reduce risk to your company in becoming a financial victim to this scam:

- The sender's email address or website link **does not** end in **.edu**. Scammers may attempt to insert an "edu" somewhere within their email address to fool you, however. **Genuine University email addresses always END in .edu**
- The emails often attempt to impersonate a UNM Purchasing staff member
- The message requests shipment of products to a non-University of New Mexico address, either to another state or to a cross-dock warehousing service.
- The email message is poorly written with misspellings and awkward sentence structure
- 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.
- The quote requests large quantities of highly resalable items such as electronics, hard drives, memory, toner cartridges, medical or scientific items, etc.

### **SUPPLIERS BEWARE! THESE FRAUDULENT EMAIL ADDRESSES ARE CURRENTLY BEING USED BY SCAMMERS TO IMPERSONATE THE UNM PURCHASING DEPARTMENT:**

<a href="mailto:rmortensen@unm-purchase.com">rmortensen@unm-purchase.com</a>	<a href="mailto:cherrin@unm-purchase.com">cherrin@unm-purchase.com</a>	<a href="mailto:rortiz09@unm-purchasing.com">rortiz09@unm-purchasing.com</a>
<a href="mailto:rmortensen@unm-purchasing.com">rmortensen@unm-purchasing.com</a>	<a href="mailto:bruce.cherrin@uninm-edu.com">bruce.cherrin@uninm-edu.com</a>	<a href="mailto:rortiz09@unm-purchase.com">rortiz09@unm-purchase.com</a>
<a href="mailto:Accounting@Uninm-edu.com">Accounting@Uninm-edu.com</a>	<a href="mailto:cherrin@unm-purchasing.com">cherrin@unm-purchasing.com</a>	<a href="mailto:purchasing@uninm-edu.us">purchasing@uninm-edu.us</a>
<a href="mailto:purchasing@unm-edu.us">purchasing@unm-edu.us</a>	<a href="mailto:bruce.cherrin@uninm-edu.com">bruce.cherrin@uninm-edu.com</a>	<a href="mailto:accounting@uninm-edu.com">accounting@uninm-edu.com</a>
<a href="mailto:purchasing@uninm-edu.net">purchasing@uninm-edu.net</a>	<a href="mailto:purchasing@unmmm.org">purchasing@unmmm.org</a>	<a href="mailto:purchasing@uninm-edu.org">purchasing@uninm-edu.org</a>
<a href="mailto:purchasing@unim-edu.us">purchasing@unim-edu.us</a>		

**\*\*\*Please note that none of the above fraudulent email addresses end in .edu**

**FRAUDULENT PHONE NUMBERS/FAX NUMBERS CURRENTLY BEING USED BY SCAMMERS:**

(505) 886-5785

(505) 212-0206

(505) 317-0219

(505) 212-1173

(505) 337-0469

(505) 300-0653

(505) 832-8777

If you believe you have received a fraudulent email that appears to be from the University of New Mexico, you may forward it to our Procurement Services department at [purch@unm.edu](mailto:purch@unm.edu) to verify its legitimacy before responding to the email or filling the order. You may also contact the UNM Procurement Services department by phone, Monday through Friday, 8:00 am to 5:00 pm MST at (505) 277-2036.