ALERT: Fraudulent Purchase Order Activity

The University's Supply Chain Services office wants to alert the University community and suppliers about a scam targeting higher education institutions. The scam involves sending suppliers purchase orders and requests for quotes that appear to originate from universities but are in fact fraudulent.

The fraudulent communications may include attachments that are designed to look like official purchase orders or requests for quotes. They may include a logo or other graphics copied from websites, or forged signatures of university employees.

We have alerted law enforcement officials.

Here are some common themes of fraudulent communications to be aware of. Recognizing these red flags may help reduce your risk of becoming a victim of this financial scam.

- The sender's message or purchase order requests shipment/delivery of products to a non-University address. Take a moment to verify the address on the University's website and a web map service, such as Google Maps. The University does not request delivery to residential addresses, storage units, warehouses, or business complexes not affiliated with the University.
- A request is made at the last minute to ship to a different address, especially one that is outside of Florida or the Miami-Dade County area.
- The message does not come from an address that is part of one of the University's standard email address domains (@miami.edu or @med.miami.edu), but instead comes from an e-mail address that ends in .org, .com, or .net.
- The phone numbers used in the communications and/or purchase orders are not valid University of Miami phone numbers. You can search the University's employee database, located at http://people.miami.edu, to confirm an employee name and phone number.

If you are a supplier and you want to verify that a communication or purchase order you have received is valid, please contact us immediately by forwarding the message to purchasing@miami.edu or by calling 305-284-5751. We encourage you to do so before responding to any communication or filling any order you are unsure about.

If your company shipped an order based on a fraudulent purchase order or received a fraudulent request for quote or purchase order, we encourage you to report the incident to your local law enforcement agency, as well as the FBI's Internet Crime Complaint Center (www.ic3.gov).