RE: Notice to Vendors - Nationwide Purchase Order Scams

We want to alert you to an active email scam targeting suppliers at hospitals and academic institutions across the country. Please take precautions so that you are not a victim of this scam.

How does the scam work?

The fraud scam involves purchase orders and requests for product quotations that purport to originate from a legitimate organization, but are in fact fraudulent.

According to the FBI and multiple institutions, the scam has several variations, but basically works like this:

- Fraudsters set up fraudulent websites and domain names almost identical to those of real organizations. They do the same to "spoof" email accounts and also use telephone spoofing techniques to make calls appear to come from the right area code.

- Next, fraudsters—posing as organization employees—email requests for quotes for merchandise to the targeted vendor. They use forged documents and communications, complete with official logos and employee names that may be associated with the organization.

- Later, the fraudsters email a purchase order to the vendor that resembles an authentic purchase order—oftentimes on what appears to be official letterhead and even containing the name of the organization's procurement manager. The purchase order instructs delivery to an address not affiliated with the legitimate organization.

- After shipping the merchandise, the vendor never receives payment and is unable to retrieve the mailed products.

What can you do?

Be vigilant in your review of purchase orders and requests for payments or services. Additionally, look out for the following characteristics of these fraudulent emails:

- The email message is poorly written, with misspellings and awkward sentence structure;

- The sender's email address or website link are not authentic to Texas Children's Hospital (e.g., the email address is from an incorrect domain such as texaschildrens.net, or contains dashes such as texas-childrens.org);
- The message requests shipment of products to non-Texas Children's Hospital addresses;
- The message requests shipment of large dollar orders;
- The telephone number in the email is bogus and is not answered by a live person.

If you believe you have received a fraudulent email that appears to be from Texas Children's Hospital, immediately forward it to Miguel Machado at mxmachad@texaschildrens.org and Javier Hernandez at jrherna1@texaschildrens.org to verify its legitimacy before responding to the email or filling the order. You should also consider filing a complaint with the FBI's Internet Crime Complaint Center: www.ic3.gov. If your company has shipped an order based on a fraudulent purchase order issued under Texas Children's Hospital's name and is facing a financial loss, immediately contact your local law enforcement agency. Texas Children's Hospital is not responsible for any loss caused by a vendor fulling a fraudulent order.

Texas Children's Hospital values its partnership with our vendors. For more information about our vendor program, please review the information available on our website at https://www.texaschildrens.org/about-us/vendors.