Dear Valued Partner,

Please be advised that Froedtert Health has discovered a possible phishing or social engineering attempt whereby Froedtert Health executives are being impersonated in e-mails, faxes, or phone calls to our suppliers. We were made aware of these activities in September of 2014 and are evolving weekly. What makes this attempt unusual is that the party was able to register the internet domain name froedters.com and other similar domains, the similarity to our domain name increases their chance of success.

This attack has resulted in numerous purchase orders that Froedtert Hospital has not initiated.

The fraudulent purchase orders indicate various shipping addresses that are changing weekly.

If your company has a Froedtert Hospital purchase order with a suspicious address or often times misspelled domains, the order is fraudulent, and we request that you do not enter the order but instead contact the Supply Chain Main line at – 414-777-1950 or email Kristin Stewart at kristin.stewart@froedtert.com with any documentation that you may have received.

This issue is serious and disruptive to all of our businesses. We appreciate your vigilance in contacting us should you have received any fraudulent orders this week. Thank you.