ATTENTION SUPPLIERS

Important notice for all existing and potential vendors to Stony Brook University

Beware of fraudulent purchase orders, request for quotes and/or credit applications from individuals impersonating the University or a University official.

About Fraudulent Activities

Better understanding common traits or themes of fraudulent activity may help reduce risk to your company.

1. **Fake Purchase Orders**: Fraudsters can create counterfeit purchase orders that mimic Stony Brook University's official documentation, using the Stony Brook name and logo. Fraudulent orders can range from high- to low-value items. These are some common traits to fraudulent Purchase Orders:
    - **Incorrect Email Domains** – the sender may generate a request from an email address or website that is not connected with the University. The University's email addresses end in "@stonybrook.edu". Hover your mouse over an email address to reveal the true email domain. Fraudulent email address examples include:
        1. **johnsmith@stonybrook-edu.org**
        2. **johnsmith.stonybrook@gmail.com**
        3. **johnsmith@stonybrook.com**
        4. **johnsmith@stonybrook.org**
    - **Incorrect Contact Information** – the sender may use a phone number that is not attached to the University. It is prudent to call the phone numbers listed on the University's website.
    - **Incorrect Bill-To or Ship-To Addresses.** A fraudulent Purchase Order will often request a shipment of product to a non-University address. Confirm the ship-to address on all purchase orders are associated with the University.
    - **Urgent Delivery Requests.** Be suspicious of any orders that require you to act immediately. This is common technique used to create a false sense of urgency, so recipients have less time to evaluate the validity of the message.
2. **Fake Credit Applications:** The University does not pay for goods using a credit application. Any request for credit applications should be reported immediately.
3. **Other indicators of fraudulent orders may include:**
    - Instructions to ship products to unfamiliar addresses (an address not associated with the University).
    - Phone numbers not associated with the University.
    - Rushed orders.
    - Payment instructions different from our standard procedures

How to Identify Fraudulent Requests

To protect your business and ensure the authenticity of any requests or orders, please consider the following guidelines:

- **Verify Contact Information**: Check that the email addresses and phone numbers match our official contact details.
- **Scrutinize Unusual Requests**: Be cautious of urgent orders that deviate from our typical purchasing patterns.
- **Confirm Orders**: Always confirm the order details with your regular procurement official at the University. Use the phone numbers or email addresses you have on file to verify the authenticity.
- **Payment Verification**: Ensure that payment instructions align with our standard processes. Do not proceed with new or unusual payment instructions without verification.

What You Should Do

If you receive a suspicious order or email purportedly from the University, please:

1. **Report Immediately**: Contact a University Procurement Official directly using the official contact details you have on file.
2. **Do Not Fulfill the Order**: Do not fill a suspicious purchase order until you have confirmed its legitimacy with a University Procurement Official.
3. **Provide Details**: Share any suspicious emails or documents with a University Procurement Official to aid in an investigation.

Contact Information

For any concerns or to report suspicious activity, please reach out to us at:

- **Compliance Contact:** Doug Panico
  - **Email**: douglas.panico@stonybrook.edu
  - **Phone**: 631.632.1439
- **Procurement Contact:** Frank Bowden
  - **Email**: frank.bowden@stonybrook.edu
  - **Phone**: 631.632.9110

Your vigilance is crucial in preventing these fraudulent activities. The University cannot prevent this illegal activity. All vendors and partners need to strictly follow their own internal business processes to protect themselves.

We value our partnership and appreciate your attention to this important matter. While the University cannot prevent this illegal activity, we can work together to ensure the integrity and security of our transactions.