

Best Practices to Combat Wire Fraud

How to detect potential wire fraud:

- ✓ Carefully examine the details of the requested wire transfer
- ✓ How and when was the request was received
- ✓ Are the payments to beneficiaries or vendors new or outside of where the business typically operates? For example, a first-time request for a wire transfer to a bank account in a foreign country.

Precautions you can take to protect your business from falling victim

- Increase awareness within your business, especially those authorizing wire transfers
- Implement a call verification process when setting up payment instructions for a new vendor or making changes to payment instructions for an existing vendor
- Implement dual control and segregation of duties
- Verify payment instructions by telephone to a previously known or verified phone number and **NEVER TO A NUMBER PROVIDED IN THE EMAIL**
- Be cautious of spoofed/mimicked email addresses
- Implement technology solutions to identify suspicious emails
 - Scan hardware for any spyware, malware, or Trojan horses etc.
 - Establish a program or rules that will raise a red flag if the name on an incoming email for not exactly match an existing contact
- Review your business insurance policy. Does it cover losses due to cybersecurity fraud?

To learn more, visit our Fraud Security Page @ www.firstbanknj.com/security