Best Practices For Businesses To Prevent Wire Transfer Fraud

Develop and adhere to company-wide policies designed to increase employee awareness and the prevention of wire transfer fraud that incorporate some of all of the following best practices:

- Requests for changes, immediate action, or lack of availability by phone should be met with intense scrutiny. Review the modified instructions in detail for any inconsistencies and always follow a call-back procedure.

- Implement a two-step verification process for all wire transfer communications. Require that employees verify wiring instructions by phone with an identified person on the other side of the wire transfer prior to initiating the wire.

- Do not email wiring instructions. Use regular mail, phone or fax instead.

- Scrutinize all email correspondence regarding wiring funds.

- Do not use public domain email accounts for business purposes. Establish company domain email accounts instead.

- Use encrypted email for correspondence of sensitive information.

- Be careful of what is posted to social media, both on behalf of the business and the individual employees of a company. Think twice before providing details on out-of-office replies, job descriptions and organizational chart information.

- Delete unsolicited spam email. Do not open spam email or click on links provided in suspicious email.

- Use extreme caution when sending wires internationally. Once money leaves the United States, it is likely gone forever.

- Forward instead of reply: Rather than reply to an email, forward the email to the address that you have on file. A common trick is to slightly modify an email address. For example, john.smith@abc.com might be changed to jon.smith@abc.com.

- The best defenses against wire fraud include rock-solid internal procedures and training team members to recognize the signs of suspicious activity within the company.