What to do if you are a victim of a Business Email Compromise Scheme

NOTE: This information is being provided to victims or potential victims of BEC schemes to ensure appropriate action is taken to try to recover the stolen funds.

A Business Email Compromise (BEC) scheme targets businesses and/or individuals performing wire transfer payments (e.g., for the payment of an invoice or purchase of real estate). These rely on social engineering and deception to convince victims to send their money, usually a wire transfer, to criminal actors and are initiated when a victim receives false wire instructions from someone masquerading as a trusted business contact. In most cases, legitimate email accounts have been spoofed or compromised to lend legitimacy to the emails purporting to be from trusted contacts.

According to the FBI's Internet Crime Complaint Center (IC3), the area covered by FBI Tampa is #2 in the country in terms of losses incurred by victims of BEC schemes. Due to the sophisticated nature of the scheme, it is critical for victims to take action **as soon as the fraud is discovered**. The FBI has established protocols for both domestic and international wire transfers.

If you are a victim of a BEC scam, please take the below actions immediately:

- ☐ **Contact your bank**
  - ☐ Determine the appropriate contact at your bank who has the authority to reverse or "recall" the wire transfer you made.
  - ☐ Ensure the bank understands you have been the victim of a Business Email Compromise.
  - ☐ Request a Wire Recall or SWIFT Recall Message
  - ☐ Request your bank to fully cooperate with law enforcement
- ☐ **Contact FBI Tampa (813-253-1000) and follow the prompts to speak with an operator**
- ☐ **Report the incident to the FBI at: www.IC3.gov**

  Be prepared to provide all details related to the transaction (date, amount, sending and receiving bank names, account numbers, contact information, etc.).

For additional information, please contact FBI Tampa at:
TP-CTOC@fbi.gov