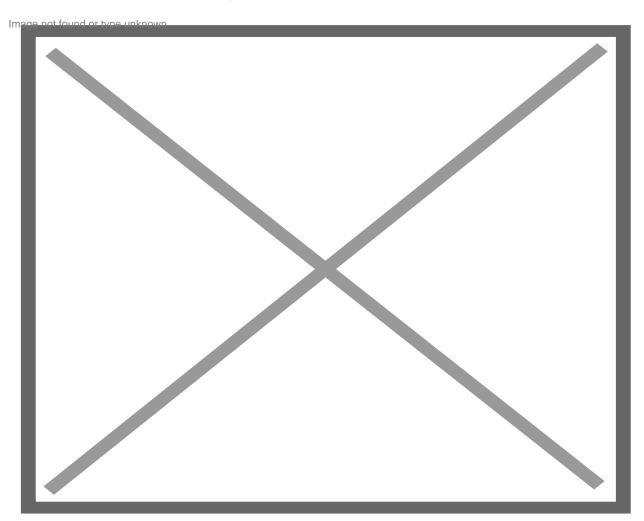# Email Scams Circulating in USVI are Forcing Local Businesses to Pay Fraudulent Invoices; Lt. Gov. Urging Vigilance

Business / **Published On December 06, 2022 07:14 AM /**

Staff Consortium December 06, 2022

Lieutenant Governor Tregenza Roach in his capacity as chairman of the V.I. Banking Board is advising business owners and their employees to be aware of Business Email Compromise (BEC) scams, which are skillfully targeting businesses in the territory and inducing them to pay fraudulent invoices.

BEC is a type of cybercrime where scammers use emails to trick an employee into sending money or divulging confidential company information, said the Office of the Lieutenant Governor. The scammer poses as a legitimate business, then asks for a fake bill, or invoice to be paid or seeking sensitive data which can be used in this scam and into the future.

"In the cases brought to our attention, scammers emulate a vendor that the company regularly does business with, by sending emails to a targeted employee requesting payment for what sounds like a legitimate purpose, such as an acquisition or vendor payment" stated Mr. Roach.

The message generally requires the employee to update data from the vendor's bank account which now allows access by the fraudster. Businesses are encouraged to stay vigilant and look out for any signs of the following:

- Slight variations on legitimate addresses.
- Seemingly legitimate emails requesting that you change payment account information for a vendor.
- Use of malware (malicious software to infiltrate company network).

A business which falls victim to a BEC scam should contact its financial institution immediately, contact the police department and local FBI field office to report the crime, and file a complaint with the FBI's Internet Crime Complaint Center.

For additional information or questions regarding BEC scams, contact the Division of Banking, Insurance, and Financial Regulation's Acting Director Glendina Matthew, Esq. at 340-773-6459.