BEWARE OF FRAUD SCHEMES DURING DISASTERS

When disaster strikes, criminals often ramp up their attacks when consumers are most vulnerable. Below are some of the types of fraud you or your business may encounter as a result of COVID-19.

Cybercrime Schemes

- **Malware**: Malicious software used by criminals to steal data or gain unauthorized access (i.e., ransomware, spyware, trojans)
- **Phishing**: Fraudulent communication, often through email, that appears to be from a legitimate sender to persuade the recipient to reveal financial data, login credentials, etc.
- **SMiShing**: Similar to phishing but uses SMS text messages to trick the recipient into revealing information
- **Spoofing**: Communication, usually emails, from an unknown source disguised as a known, legitimate source, often financial institutions

Investment Fraud

- Be aware of pump-and-dump penny stocks for companies purporting cures to COVID-19.
- Use extreme caution with companies that claim fake celebrity endorsements of products, especially products related to COVID-19.
- On February 4, 2020, the U.S. Securities and Exchange Commission (SEC) issued an Investor Alert related to COVID-19:

  "We have become aware of a number of Internet promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect, or cure coronavirus, and that the stock of these companies will dramatically increase in value as a result. …These claims may be made as part of fraudulent 'pump-and-dump' schemes."

Payment and Corporate Fraud

- **Wire transfer redirection**: often in Business Compromise Emails (BEC), emails appearing as a colleague or supervisor that seek the recipient to quickly send payment or other confidential information such as W2s
- **Payroll Schemes**: payments to ghost employees and time-card fraud
- **Expense Fraud**: fraudulent expense reimbursements to employees
- **Vendor Fraud**: fraudulent cash disbursement by employees to fake vendors
- **Asset Misappropriation**: theft or misuse of company assets by employees

Charity Fraud

- During disasters, some criminals create fake charities or crowdfunding sites, such as GoFundMe, to solicit donations for non-existent charities or situations.
- How to protect yourself from becoming a victim:
  - Do your homework and verify charities through sites like Charity Navigator
  - Choose your payment method wisely by paying by credit card or check. Beware of charities seeking payment by cash, gift cards, wires or bitcoin.

For more information and assistance, or if you believe your company has encountered fraud, please contact Natalie Lewis, nlewis@windhambrannon.com or 678-510-2801.

WINDHAM BRANNON
offering more