LAW ALERT

April 9, 2020

By: Jay B. Silverman, Esq.

RMF
RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

FBI Warns of COVID-19 Scams

On April 6, 2020, the Federal Bureau of Investigations ("FBI") issued an alert warning of an increase in Business Email Compromise ("BEC") scammers who are targeting individuals and companies making legitimate funds transfers. In a BEC scheme, a victim receives an email believed to be from someone the person or company regularly does business with, however, in the email the scammer directs that the funds be sent to a new account or changes the standard payment practices.

According to the FBI alert, recent examples of BEC scams include a financial institution that received an email allegedly from the CEO of a company, who had previously scheduled a transfer of $1 million, requesting that the transfer date be moved up and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions." The email address used by the scammers was almost identical to the CEO's actual email address with only one letter changed. The FBI cites another example where a bank customer received an email from someone claiming to be one of the bank customer's clients in China. The scammer requested that all invoice payments be changed to a different bank because their regular bank accounts were inaccessible due to "Corona Virus audits." Unfortunately, the victim sent several wires to the new bank account before discovering the fraud.

To protect against BEC scams, the FBI advises that individuals and companies be on the lookout for certain red flags such as:

- unexplained urgency;
- last minute changes in wire instructions or recipient account information;
- last minute changes in established methods of communication or email addresses;
- communications only in email and refusal to communicate by phone or other methods;
- requests for advanced payment of services when not previously required; and
- requests from employees to change direct deposit information.

The FBI also advises individuals and companies to:

- be skeptical of last minute changes in wiring instructions or recipient account information;
- verify any changes and not contact the vendor through the number provided in the email;
- ensure the URL in emails is associated with the business it claims to be from;
- be alert to hyperlinks that may contain misspellings of the actual domain name; and
- verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match whom it is coming from.

Finally, the FBI advises that should you discover that you or your company have been the victim of BEC fraud, immediately contact your financial institution to request a recall of funds and an employer to report any irregularities with payroll deposits. Complaints can be filed with the FBI's Internet Crime Complaint Center at ic3.gov or, for BEC and/or email account compromise (EAC) victims, bec.ic3.gov.

If you have any questions, please contact
Jay B. Silverman, Esq.
(516) 663-6606
jsilverman@rmfpc.com