> Covid-19 Client Alert

FBI Issues Broad Warning of Surge of COVID-19 Scams

April 14, 2020

Authors and Key Contacts

If you have any questions about this alert, please contact any of the attorneys listed below.

Joseph T. Moldovan
Partner & Chair,
Business Solutions, Restructuring & Governance Practice
P (212) 735-8603
F (917) 522-3103
jmoldovan@morrisoncohen.com

David Lerner
Partner,
Technology, Data Privacy & Intellectual Property Practice
P (212) 735-8609
F (917) 522-3109
dlerner@morrisoncohen.com

Recognizing that cybercriminals are turning their attention to a nation largely and suddenly working remotely from home during the COVID-19 pandemic, the FBI this week issued a broad warning that Americans should expect and be on guard for a surge in electronic extortion, treatment fraud, and cryptocurrency schemes.

The FBI's warning highlighted a variety of traditional and new scams racing through the country, seeking to take advantage of the substantially greater use of home computer systems which are typically less secure than those used at work, along with reduced direct employer oversight, coupled with the general fear and confusion sown by the pandemic. Among the swindles identified in the warning include:

- bogus COVID-19 treatments, equipment or preventions appearing to come from legitimate e-commerce sites;
- malware attacks demanding the payment of ransom in untraceable cryptocurrency such as Bitcoin to allow the victim to recover stolen data or to avoid the disclosure of private information;
- phishing attacks falsely appearing to originate from the employer seeking the employee's banking information and directing the employee to pay some amount, or, equally likely, to "receive" stolen funds (which exposes the recipient to possible liability as a money launderer); and
- garden variety securities, Medicare and charity frauds.

The Bureau advised that home-computer users should take particular care and approach any request for information or money with great skepticism, and contact law enforcement upon receiving a ransom demand.

Although not addressed by the Bureau, businesses should be particularly vigilant during the pandemic dislocation and ensure that employees at every level of the organization only have the ability to access the company's information systems through a securely controlled virtual private network, utilizing two-factor authentication and all other cybersecurity policies that operate during regular in-office operations.

* * * * * *

Morrison Cohen LLP has also created the COVID-19 Resource Taskforce, a multidisciplinary taskforce comprised of attorneys with deep expertise in a broad range of legal areas, to assist clients navigating the challenging and uncertain business and legal environment caused by the COVID-19 pandemic. We encourage clients to utilize our capabilities by reaching out to their primary Morrison Cohen attorney contact, who will put you in touch with the appropriate Taskforce person. You may also reach out directly to Joe Moldovan and Alec Nealon, the Taskforce co-chairs:

Joseph T. Moldovan
Chair, Business Solutions, Restructuring & Governance Practice
Co-Chair COVID-19 Taskforce
P (212) 735-8603
C (917) 693-9682
F (917) 522-3103
jmoldovan@morrisoncohen.com

Alec Nealon
Partner, Executive Compensation & Employee Benefits Practice
Co-Chair COVID-19 Taskforce
P (212) 735-8878
C (646) 318-4845
F (917) 522-9978
anealon@morrisoncohen.com