# DOJ is Aggressively Investigating Allegations of Wrongdoing Related to COVID-19 Fraud and the Current National Emergency


**(March 27, 2019):** We live in trying times. As the coronavirus disease (COVID-19) has spread both globally and throughout the United States, the government has taken a number of steps to address the current pandemic. On March 13, 2020, President Donald Trump officially declared that the COVID-19 outbreak constitutes a national emergency.[1] Within 72 hours of the issuance of President Trump's declaration, William Barr, the Attorney General of the United States, determined it was necessary to issue a memorandum to the 94 U.S. Attorney's Offices around the country stressing the fact that Department of Justice (DOJ) prosecutors must remain diligent in their efforts to detect, investigate and prosecute wrongdoing related to the COVID-19 crisis. This article examines the various COVID-19 fraud concerns that DOJ has already raised and sets out steps you can take to reduce your level of regulatory risk.

## I. Overview of DOJ Guidance of COVID-19 Fraud and Related Wrongdoing:

As mentioned above, on March 16, 2020, the Attorney General issued guidance**[2]** to the 94 U.S. Attorney's Office around the country noting that it is essential that the justice system remain functioning throughout the national emergency. It is also worth noting that U.S. Attorney's Offices has been ***"directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic."***

Less than a week after issuing this initial guidance, the DOJ announced on Sunday, March 22, 2020, that it had filed its first enforcement action in the Western District of Texas related to COVID-19 fraud. As set out in the Civil Complaint filed by the government, the defendants have been alleged to have engaged in a ***"wire fraud scheme seeking to profit from the confusion and widespread fear surrounding COVID-19"*** through the company's sale of World Health Organization (WHO) vaccine kits. As the government notes, at this time, there are no legitimate COVID-19 vaccines and the WHO is not distributing such a vaccine. As Assistant Attorney General Jody Hunt of the Department of Justice's Civil Division stated at the time:

> ***"The Department of Justice will not tolerate criminal exploitation of this national emergency for personal gain . . . We will use every resource at the government's***

> ***disposal to act quickly to shut down these most despicable of scammers, whether they are defrauding consumers, committing identity theft, or delivering malware."***[3]

Even more recently, on March 25, 2020, the U.S. Attorney's Office for the Central District of California announced that it had filed a criminal complaint against an individual who allegedly solicited investments in a company that was marketing pills that would prevent coronavirus infections. The defendant's company was also supposedly marketing an injectable cure for individuals battling COVID-19. The complaint charges the individual with a single count of attempted wire fraud. **[9]**

## II. Specific Guidance Issued by Deputy Attorney Rosen on COVID-19 Fraud:

Shortly thereafter, on March 25, 2020, Deputy Attorney General, Jeffrey A. Rosen issued guidance titled ***"Department of Justice Enforcement Actions Related to COVID-19."*** [4] As the guidance notes, there are a number of specific statutory authorities that Federal prosecutors may find applies to assert if COVID-19 fraud or wrongdoing is identified. These statutory authorities include, but are not limited to:

**Federal Statutory Authority**

**15 U.S.C. § 1 -- Trusts, etc. in Restraint of Trade Illegal; Penalty**
**15 U.S.C. § 2 – Monopolizing Trade a Felony; Penalty**
**15 U.S.C. § 14 – Sale etc., on Agreement not to Use Goods of Competitor**
**15 U.S.C. § 1263 – Prohibited Acts (Introduction of Misbranded or Banned Hazardous Substances into Interstate Commerce)**
**15 U.S.C. § 2068 – Prohibited Acts (Sale, Manufacture, Distribution or Import of a Consumer Product or other Product that is not in Conformity with Consumer-Product-Safety Regulations)**
**18 U.S.C. § 175 -- Prohibitions with Respect to Biological Weapons**
**18 U.S.C. § 875 -- Interstate Communications**
**18 U.S.C. § 876 – Mailing Threatening Communications**
**18 U.S.C. § 1030 -- Fraud and Related Activity in Connection with Computers**
**18 U.S.C. § 1038 -- False Information and Hoaxes**
**18 U.S.C. § 1040 -- Fraud in Connection with Major Disasters and Emergencies**
**18 U.S.C. § 1341 – Frauds and Swindles (Mail Fraud)**
**18 U.S.C. § 1343 – Fraud by Wire, Radio or Television (Wire Fraud)**
**18 U.S.C. § 1347 -- Healthcare Fraud**
**18 U.S.C. § 1349 -- Conspiracy to Commit Fraud**
**18 U.S.C. §§ 1028-1028A -- Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information (Identification Fraud and Aggravated Identity Theft)**
**18 U.S.C. § 2320 --Trafficking in Counterfeit Goods**

**18 U.S.C. § 2332a -- Use of Weapons of Mass Destruction**
**21 U.S.C. § 333 -- Violation of the Food, Drug, and Cosmetic Act**

Specific examples of possible COVID-19 fraud schemes that might be perpetrated were set out in Deputy Attorney General Rosen's memorandum. These examples included:

- **Robocalls making fraudulent offers to sell respirator masks with no intent of delivery. 18 U.S.C. § 1343 (Wire Fraud). The crime of "wire fraud" occurs when someone voluntarily and intentionally uses makes an interstate telephone call or another electronic communication (such as e-mail) in furtherance of a fraud scheme. Notably, the elements of wire fraud are very similar to those of mail fraud statute except that it speaks of communications transmitted by wire.**

- **Fake COVID-19-related apps and websites that install malware or ransomware. 18 U.S.C. § 1343 (Wire Fraud) or 18 U.S.C. § 1030 (Computer Fraud). The crime of wire fraud is described above. The crime of computer fraud occurs when someone knowingly causes the transmission of a "program, information, code or command" and intentionally damages (without authorization) a protected computer.**

- **Phishing emails asking for money or presenting malware. 18 U.S.C. § 1030 (Computer Fraud). One of the forms of computer fraud is set out above. Additional examples are also discussed under 18 U.S.C. § 1030.[5]**

- **Social media scams fraudulently seeking donations or claiming to provide stimulus funds if the recipient enters his or her bank account number. 18 U.S.C. §§ 1028-1028A (Identity Theft) or 18 U.S.C. § 1343 (Wire Fraud). Notably, the government has extensive experience prosecuting individuals and entities who are alleged to have set up fake charities and have effectively taken advantage of a national disaster or tragedy. The perpetrators of this type of fraud are almost always caught and the courts have levied heavy jail sentences and fines on bad actors found guilty of engaging in this type of wrongdoing.**

- **Sales of fake testing kits, cures, "immunity" pills, and protective equipment. 21 U.S.C. 333 (Introduction of Misbranded or Adulterated Drug or Device Into Interstate Commerce) or 15 U.S.C. § 2068 (Violation of the Consumer Product Safety Act). Federal prosecutors and regulators for the Food and Drug Administration (FDA) handle these types of cases on an ongoing basis and are experienced in shutting down fraudsters hawking fake cures and treatments.**

- **Fraudulent offers for free COVID-19 testing in order to obtain Medicare beneficiary information that is used to submit false medical claims for unrelated, unnecessary, or fictitious testing or services. 18 U.S.C. §§ 1028-1028A (Identification Fraud and Aggravated Identity Theft). This type of fraud has been occurring law before the inception of the COVID-19 fraud cases we are now seeing. Most recently, Medicare beneficiary information has been misused by a number of telemarketing companies and durable medical equipment companies. Federal prosecutors are currently in the middle of several prosecutions involving this type of conduct.**

- **Prescription drug schemes involving the submission of medical claims for unnecessary antiretroviral treatments or other drugs that are marketed as purported cures for COVID19. 18 U.S.C. § 1347 (Healthcare Fraud) or 15 U.S.C. § 2068 (Violation of the Consumer Product Safety Act). These common schemes are now being seen in connection with COVID-19 fraud cases around the country. Health care providers should exercise caution before entering into business relationships with laboratories, pharmacies and other ancillary service providers who are marketing purported cures or treatment regimens for COVID-19.**

- **Robberies of patients departing from hospitals or doctor offices. 18 U.S.C. § 2118 (Robberies and Burglaries Involving Controlled Substances). Although not discussed in Deputy Attorney General Rosen's memorandum, it is a Federal crime to take, or attempt to take, by force or violence or by intimidation, any quantity of a controlled substance from any person (including a patient) on the business premises or property of a person registered with the Drug Enforcement Administration. In addition, to this Federal statute, there are a host of robbery statutes that would implicated under State law.**

- **Threats of violence against mayors and other public officials. 18 U.S.C. § 875 (Interstate Communications) or 18 U.S.C. § 876 (Mailing Threatening Communications). Using the internet to convey an interstate threat of violence or injury to any person would be a crime under 18 U.S.C. § 875. Similarly, using the mails to threaten someone with violence or injury would be a crime under 18 U.S.C. § 876.**

- **Threats to intentionally infect other people. 18 U.S.C. § 2332a (Use of Weapons of Mass Destruction). Of the examples discussed in Deputy Attorney General Rosen's guidance, this is perhaps the most interesting. As the memorandum reflects, Federal prosecutors may view "*Threats or attempts to use COVID-19 as a weapon against Americans*" as a violation of 18 U.S.C.**

**§ 2332a since COVID-19 arguably meets the statutory definition of a *"biological agent"* [6]and therefore could implicate our country's terrorism-related statutes.**

## III. Reducing Your Level of Regulatory Risk During the Current National Emergency:

Although the health, societal and business impact of the current COVID-19 emergency is unprecedented (at least in our lifetime), the fact that bad actors will readily take advantage of this situation is to be expected. In fact, with the exception of the terroristic threat conduct discussed above, the types of wrongdoing encountered in COVID-19 fraud cases is pretty run-of-the-mill. In addition to the concerns raised in Deputy Attorney General Rosen's memorandum, several additional areas of risk to be considered by health care providers and suppliers include the following:

- **Exercise Due Diligence Before Accepting the Assertions of Medicare Coverage by a Vendor's Sales Representative. There are a wide variety of medical devices and pharmaceutical products that have not been properly vetted through the FDA approval process in order to qualify for coverage and payment by Medicare. Don't assume that sales pitches asserting that a medical device or pharmaceutical product is correct. In recent years, we have represented multiple providers who were talked into buying expensive equipment and other products based on a sales representatives promises that the item or service to be billed qualifies for Medicare coverage and payment. In once case we handled, when our client was audited, the company that sold the medical device at issue had long since gone out of business and had been sued by other providers for misrepresenting that the services performed with the medical device could be properly billed to Medicare.**
- **Take Care if You Seek a Bank or Small Business Administration (SBA) Loan as a Result of the COVID-19 Crisis. In an effort to help businesses deal with the current national emergency, the government has streamlined the SBA loan process for small businesses. Two recent articles[7]covering these developments have been placed on our website. Should you decide to seek a bank or SBA backed business loan, you must exercise care when completing these applications. While the documentation and approval timeframes may have been simplified, should you make a misstatement on the application or fail to disclose relevant information, your actions may constitute a crime.**
- **Government Waivers of Certain Requirements (Such as those Associated with Telehealth / Telemedicine Services) are Always Limited. To its credit, the**

> **Centers for Medicare and Medicare Services (CMS) have been quick to address many of the patient access, diagnostic and treatment concerns expressed by health care providers and patients alike that have arisen because of the current COVID-19 outbreak. For example, CMS maintains a list of services that are normally furnished in-person that it will now permit providers to furnish by Medicare telehealth. As CMS wrote in recent guidance[8] it issued on March 17, 2020: *"Under the emergency declaration and waivers, these services may be provided to patients by professionals regardless of patient location."* Don't assume that the relaxation of Medicare's telehealth / telemedicine rules are an indication that this area is no longer under extreme scrutiny by law enforcement and by CMS program integrity contractors such as Unified Program Integrity Contractors (UPICs). Once our country has effectively dealt with the current national emergency, government investigators and CMS contractors will undoubtedly resume their review and audit of these historically-problematic claims. For a more detailed discussion of the government's enforcement efforts in this regard, please see our article from February 17, 2020, titled *"Telemedicine Audits of Evaluations by Referring Physicians are Increasing."***

While CMS is continuing to identify additional ways that it can better facilitate the provision of patient care, health care providers need to remember that specific waivers recently approved by CMS are likely to be short-term in nature. More importantly, all other coverage and payment requirements remain in effect. First and foremost, were the services medically necessary? Were the services properly documented (in accordance with CMS, State Medical Board and Industry Standards)? Were the services properly coded and billed? And finally, was the reimbursement you received accurate?

Once the current national emergency is over, health care providers and suppliers should expect to see significant upswings in program integrity audits by Unified Program Integrity Contractors (UPICs), Supplemental Medical Review Contractors (SMRCs) and Comprehensive Error Rate Testing (CERT) contractors. As this health crisis continues, it is also important to keep in mind that State and Federal law enforcement agencies are actively soliciting reports of COVID-19 fraud and other related wrongdoing. Attorney General Barr has urged the public to report any and all COVID-19 fraud schemes that are identified to the ***National Center for Disaster Fraud*** (NCDF) hotline. As a result, it is imperative that you continue to ensure that your regulatory compliance efforts are both ongoing and up-to-date (in terms of your obligations under the law).

Have you received a document request from the OIG, a UPIC, a SMRC or another CMS contractor? Are you currently facing a government audit or investigation of your claims billed to

Medicare, Medicaid or another Federal health benefit program? **Call us for a free consultation. We can be reached at: (202) 298-8750 or toll-free 1 (800) 475-1906.**

**Robert W. Liles serves as Managing Partner at the health law firm, Liles Parker, Attorneys and Counselors at Law. Liles Parker attorneys represent health care providers and suppliers around the country in connection with claims audits and investigation. Is your health care practice, home health agency or hospice being audited? Give us a call. *For a free initial consultation regarding your situation, call Robert at:* 1 (800) 475-1906.**

**[1]** ***"Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak*,"**dated March 13, 2020. A copy of the declaration can be found the following **link.**

**[2]** DOJ's Memorandum, ***"COVID-19 – Department of Justice Priorities,"*** March 16, 2020. A copy can be found at the following **link.**

[3] A copy of DOJ's Press Release is available at this **link**.

**[4]** DOJ's Memorandum, ***"Department of Justice Enforcement Actions Related to COVIF-19,"*** *March 24, 2020.* A copy can be found at the following **link.**

**[5]** 18 U.S.C. § 1030 (Fraud and Related Activity in Connection with Computers). A link to the statute can be found **here.**

**[6]** See 18 U.S.C. § 175.

**[7]** Our article titled ***"Small Business Administration Releases Express Bridge Loan Pilot Program for COVID-19,"*** dated March 26, 2020, can be found **here**. An earlier article titled ***"COVID-19 SBA Loan Support May be Available for Qualified Health Care Providers,"*** dated March 25, 2020, can be found **here.**

**[8]** CMS guidance titled ***"Medicare Telehealth Frequently Asked Questions (FAQs),"*** dated March 17, 2020, can be found **here.**

**[9]** A copy of the Press Release can be found here.