

## COVID-19 AND FRAUD: DOJ PURSUES ENFORCEMENT ACTION AND OIG ISSUES FRAUD ALERT

As the country contends with exponential growth in the number of Coronavirus Disease 2019 (“COVID-19”) cases, government agencies tasked with protecting health care programs and enforcing the law are sending strong messages to those who may commit fraud to take advantage of the current situation. The U.S. Department of Justice (“DOJ”) filed an enforcement action against operators of a COVID-19 website for engaging in a wire fraud scheme, and the U.S. Department of Health and Human Services (“HHS”) Office of Inspector General (“OIG”) issued a Fraud Alert with warnings about Medicare fraud related to COVID-19, including scammers offering COVID-19 tests and requesting personal information.

Both **DOJ** and **OIG** encourage reporting of suspected schemes related to COVID-19 that could target and victimize individuals who are already in a vulnerable position because of anxiety amidst the public health emergency, underlying health conditions or other reasons. Health care providers, entities and anyone else that suspects COVID-19 fraud should contact the National Center for Disaster Fraud (“NCDF”) hotline at (866) 720-5721 or [disaster@leo.gov](mailto:disaster@leo.gov). NCDF maintains complaints in a manner accessible to DOJ and U.S. Attorneys’ offices, and it also coordinates complaints with 16 other federal law enforcement agencies, as well as state and local authorities.

### DOJ FILES ITS FIRST ENFORCEMENT ACTION AGAINST COVID-19 FRAUD

On March 22, 2020, DOJ announced in a [press release](#) that it filed its first enforcement action related to COVID-19 in Austin, Texas against operators of a fraudulent website, [coronavirusmedicalkit.com](http://coronavirusmedicalkit.com), which claimed that the World Health Organization (“WHO”) provided free COVID-19 vaccine kits and offered those kits in exchange for a shipping charge of \$4.95 to be paid by credit card. In response to DOJ’s allegation of wire fraud and request for action, the judge issued a temporary restraining order against the website’s registrar while the investigation continues.

The press release also contains suggested precautionary measures to protect individuals from fraudulent scams related to COVID-19. This follows an announcement from U.S. Attorney General William P. Barr directing all U.S. Attorneys to prioritize investigating and prosecuting COVID-19 fraud. Deputy Attorney General Jeffrey Rosen also issued a memorandum instructing each U.S. Attorney to appoint a Coronavirus Fraud Coordinator to serve as the primary legal counsel on matters relating to COVID-19, direct the prosecution of COVID-19-related crimes, and conduct outreach and awareness. Already, DOJ has encountered schemes including:

- Medical providers obtaining patient information for COVID-19 testing and using that information to fraudulently bill for other tests and procedures;
- The sale of fake cures for COVID-19 online;
- Phishing emails from entities posing as COVID-19 information sources such as WHO and the Centers for Disease Control and Prevention;
- Malicious websites and apps that appear to share COVID-19 information to gain and lock access to your devices until payment is received; and
- Requests for donations for illegitimate or non-existent charitable organizations.

Additional DOJ resources related to COVID-19 are located [here](#).

### OIG ISSUES COVID-19 FRAUD ALERT

On March 23, 2020, OIG released a **COVID-19 Fraud Alert** and **message** with warnings about fraudulent health care schemes targeting Medicare beneficiaries. Specifically, OIG announced that scammers are “offering COVID-19 tests to Medicare beneficiaries in exchange for personal details, including Medicare information.” OIG emphasized its commitment to protecting beneficiaries and exercising vigilance in investigation and enforcement.

OIG announced that bad actors marketed fake COVID-19 test kits and unapproved treatments through telemarketing calls, social media

platforms and other means. For instance, some fraudsters impersonating Red Cross volunteers even made door-to-door visits offering COVID-19 tests. OIG noted that some scammers requested personal information from Medicare beneficiaries which could be used to fraudulently bill federal health care programs or commit medical identity theft. Stating that such unapproved, illegitimate actions could leave beneficiaries responsible for costs for services that they did not receive, OIG cautioned against responding to requests for personal information. The Fraud Alert, accompanied by a video with guidance, provides suggestions for how Medicare beneficiaries may protect themselves and avoid becoming a victim of fraud. This guidance includes the following:

- Be cautious of unsolicited requests for beneficiaries' Medicare or Medicaid identification numbers;
- Be suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies, and note that compromised personal information could be used in other fraud schemes;
- Be wary of offers or advertisements for COVID-19 testing or treatment; and
- Make sure that a physician or other trusted health care provider assesses medical conditions and approves any requests for COVID-19 tests.

## PRACTICAL TAKEAWAYS

Despite the national emergency associated with COVID-19, fraud investigation and enforcement remain priorities for the federal government. Health care entities should be aware of these types of fraudulent schemes and caution patients against responding to any such solicitations or requests for personal information. Consider reminding patients that important information about testing, vaccines and treatment will come from health care providers and not through e-mail, online advertisements or unsolicited sale pitches. Health care providers and entities can also play a role in urging patients who suspect fraud or who were victims of fraud to report schemes to DOJ and OIG at the NCDF hotline or email. **Senior Medical Patrol**, which is funded by grants from HHS, tracks COVID-19 fraud and provides additional advice about reporting suspected fraud.

If you have any questions or would like additional information about this topic, please contact:

- **Scott Taebel** at [staebel@hallrender.com](mailto:staebel@hallrender.com) or (414) 721-0445;
- **Katherine Kuchan** at [kkuchan@hallrender.com](mailto:kkuchan@hallrender.com) or (414) 721-0479;
- **Adele Merenstein** at [amerenstein@hallrender.com](mailto:amerenstein@hallrender.com) or (317) 752-4427;
- **Kristen Chang** at [kchang@hallrender.com](mailto:kchang@hallrender.com) (414) 721-0923; or
- Your regular Hall Render attorney.