



Resources to Combat Coronavirus (COVID-19) Fraud

April 8, 2020

To our Florida health care industry partners,

On March 13, 2020, President Donald J. Trump declared the outbreak of Coronavirus (COVID-19) in the United States to be a national emergency. Unfortunately, criminals are now attempting to exploit COVID-19 worldwide through a variety of scams. The Department of Justice and our law enforcement partners remain vigilant in detecting, investigating, and prosecuting wrongdoing related to the crisis. Please review the following resources and guidance to help protect your organization and employees.

FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment (3/27/20)

The FBI has issued a warning to health care professionals of an increased potential for fraudulent activity dealing with the purchase of COVID-19-related medical equipment. Additionally, the FBI urges everyone to be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19. Be alert to counterfeit products and be on the lookout for suspicious activity. Learn more: <https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-health-care-professionals-of-increased-potential-for-fraudulent-sales-of-covid-19-related-medical-equipment>

Cyber Actors Take Advantage of Covid-19 Pandemic to Exploit Increased Use of Virtual Environments (4/1/20)

The FBI advises organizations and individuals to carefully consider the applications used for teleworking including video conferencing software and voice over Internet Protocol (VOIP) conference call systems. Cyber actors exploit vulnerabilities in these systems to steal sensitive information, target individuals and businesses performing financial transactions, and engage in extortion. Learn more: <https://www.ic3.gov/media/2020/200401.aspx>

FBI Sees Rise in Fraud Schemes Related to the Coronavirus (Covid-19) Pandemic (3/20/20)

Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received. Learn more: <https://www.ic3.gov/media/2020/200320.aspx>

OTHER - The Department of Justice has also warned of the following scams:

- **Treatment scams:** Scammers selling fake vaccines, medicines, and cures for COVID-19.
- **Supply scams:** Scammers are claiming they have in-demand products, like cleaning, household, health, and medical supplies, but when an order is placed, the scammer takes the money and never delivers the order.
- **Charity scams:** Scammers are fraudulently soliciting donations for non-existent charities to help people affected by the COVID-19 crisis. Scammers often use names that are similar to the names of real charities.
- **Phishing scams:** Scammers, posing as national and global health authorities, such as the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending fake emails or texts to trick the recipient into sharing their personal information like account numbers, Social Security numbers, or login IDs and passwords.
- **App scams:** Scammers are creating COVID-19 related apps that contain malware designed to steal the user's personal information after it is downloaded.
- **Provider scams:** Scammers pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demand payment for that treatment.
- **Investment scams:** Scammers are promoting the stock of small companies, which have limited publicly available information, using false or misleading claims that the companies' stock will increase dramatically due to the COVID-19 outbreak, such as claims that a company can prevent, detect, or cure COVID-19.

OFFICIAL COVID-19 INFORMATION WEBSITES

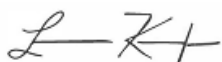
- Department of Justice - [justice.gov/coronavirus](https://www.justice.gov/coronavirus)
- Federal Bureau of Investigation - <https://www.fbi.gov/coronavirus>
- Centers for Disease Control - [coronavirus.gov](https://www.coronavirus.gov) and [cdc.gov/coronavirus](https://www.cdc.gov/coronavirus)
- Federal Government - [usa.gov/coronavirus](https://www.usa.gov/coronavirus)
- HHS-OIG – <https://oig.hhs.gov/coronavirus/>
- U.S. Immigration and Customs Enforcement – <https://www.ice.gov/coronavirus>

FILE A REPORT - If you see COVID-19 fraud being attempted or if you are a victim, contact:

- **FBI Jacksonville** – 1-800-CALL-FBI, <https://tips.fbi.gov/>, IC3 Cyber Tip Line: <https://www.ic3.gov/default.aspx>
- **United States Attorney's Office, Northern District of Florida** - COVID-19 Fraud Coordinator Assistant U.S. Attorney Justin Keen, Justin.Keen@usdoj.gov
- **HHS-OIG National Hotline** – 1-800-HHS-TIPS, <https://oig.hhs.gov>
- **DHS, Homeland Security Investigations** – 1-866-DHS-2-ICE, Covid19Fraud@dhs.gov
- **National Center for Disaster Fraud (NCDF)** – 1-866-720-5721, disaster@leo.gov

Thank you for the important work that you are doing for all of us. Please know that our teams of investigators are also working to protect you throughout this crisis.

In partnership,



Lawrence Keefe
United States Attorney
Northern District of Florida



Rachel L. Rojas
Special Agent in Charge
FBI Jacksonville



Omar Perez Aybar
Special Agent in Charge
HHS – OIG Miami



Kevin Sibley
Special Agent in Charge (Acting)
HSI Tampa