# ALERT NOTICE: Fraud Awareness During the COVID-19 National Emergency

## Beware of Fraud During the Coronavirus Public Health Emergency

As managing COVID-19 becomes part of the daily operations at health centers, procuring supplies and services related to patient treatment and response will increase. This Alert Notice is meant to bring awareness to potential fraudulent schemes that could arise during this time and assist health centers with the information they need to know to remain vigilant. Categories of scams include, but are not limited to, cyber and telemarketing fraud, high-demand product scams and price gouging, and fraud perpetrated by simulating government or other organizations.

### Cyber and Telemarketing Fraud
- Increased robocalls and fraudulent telemarketing
- Phishing emails from entities falsely claiming to be the World Health Organization or the Centers for Disease Control and Prevention
- Fake emails that appear to come from co-workers or company IT directing wiring of money, transfer of funds, or the like
- Malicious websites and apps offering COVID-19 information may infect your IT systems

### High-Demand Product Offers and Price Gouging
- Sale of fake cures, vaccinations, or treatments
- Offers of home test kits
- Online offers for in-demand supplies, like cleaning, and health and medical supplies
- Price gouging of products in demand
- Fraudulent vendors offering products in demand and never delivering
- Offer of tests or supplies to Medicare/Medicaid beneficiaries in exchange for personal details, including Medicare or Medicaid information

### Scams Simulating Legitimate Government and Organizations
- New health insurance offers
- Offers of checks or funding, claiming to be from the government
- Offers to work-at-home and earn income
- Donation requests from illegitimate or non-existence charities
- Mortgage scams claiming reduced rates
- Social Security Administration scams
- Small business listing scams

## Stay informed about and avoid fraudsters in your jurisdiction
Numerous federal and state agencies have put out alerts regarding a variety of fraud schemes. You can learn about alleged fraud in your community [here](#). Active cases include:

- Missouri Attorney General issued a [temporary restraining order](#) to stop its sale of “Silver Solution” as a treatment for COVID-19.
- Florida Attorney General [issued more than 40 subpoenas](#) against sellers over price gouging.
- Michigan Attorney General [Issues](#) Cease and Desist Letter to Businesses Selling Fake Patches
- Michigan Attorney General [Issues](#) Cease and Desist Letter to Menard’s regarding sale of cleaning products and face masks
- Michigan Attorney General [Issues](#) Cease and Desist Letter to A.M. Cleaning & Supplies
- Missouri Attorney General [Issues](#) Cease and Desist Letter to Man Selling N95 Face Masks
- New York Attorney General [Orders](#) Allyn Wayne Root to Stop Selling Fake Coronavirus Treatments
- New York Attorney General [Orders](#) Alex Jones to Stop Selling Fake Coronavirus Treatments
- New York Attorney General [Orders](#) Companies to Stop Selling Fake Coronavirus Treatments

**Protect yourself, your organization and the community you serve**

- Beware of false and misleading information that could impact you, your employees, or patients
- Beware of suspicious phone calls, emails or texts
- Beware of fraudulent charities or solicitations
- Watch out for high-priced or low-quality products
- Health centers should inform employees of fraud risk and data security risk
- Create new policies and procedures for the teleworking environment, if those do not exist
- Remind employees not to click on any unknown emails, links or websites
- Be wary of online purchases and new or unknown vendors
- Be wary of communications claiming to be from or on behalf of governments or charities
- If you are contacted by someone promising to get approval of a loan or grant but requiring any payment upfront or a high interest bridge, suspect fraud
- If you are in the process of a vendor purchase, grant or loan application and you receive a request to submit information through a link, check to ensure the email is legitimate before responding

**Report Fraud**

Contact [National Center for Disaster Fraud Hotline](#) (866) 720-5721 (disaster@leo.gov)

or

[File a complaint](#) with your State Attorney General.

This project is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of an award totaling $6,375,000 financed with non-governmental sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by HRSA, HHS, or the U.S. Government. For more information, please visit [HRSA.gov](#)