# DOJ Takes First Enforcement Action Against COVID-19 Fraud

## By Richard Kusserow | March 26, 2020

### Temporary Restraining Order issued against website offering fraudulent vaccine.

The Department of Justice (DOJ) has taken its first enforcement action in federal court to combat fraud relating to the Coronavirus (COVID-19) pandemic. The DOJ filed an action in Austin, Texas, against operators of a fraudulent website, "coronavirusmedicalkit.com," for engaging in a wire fraud scheme in order to profit from the fear and confusion around COVID-19. The website provided consumers with information on how to access and purchase World Health Organization (WHO) vaccine kits, even though there are currently no legitimate vaccines for coronavirus or COVID-19. On the website, consumers would need to use their credit card information to pay a shipping charge of $4.95 to receive the kit. The website even provided instructions on how to ensure the vaccine is ready for use by combining the two parts of the vaccine kit with water. The website stated that the two parts included: pellets containing the chemical machinery that synthesizes the end product, and pellets containing instructions that tell the drug which compound to create. The government filed the action to have the website immediately blocked from public view while it further investigates the website and its operators. In response, a federal judge issued a temporary restraining order (TRO) requiring that the registrar of the fraudulent website to immediately take action and block public access to the site. The government, in asking the court to issue a TRO, is using its authority under a federal statute that allows courts to issue injunctions to prevent harm to potential victims of fraudulent schemes.

In its announcement, the DOJ provided precautionary measures for the public to take to protect themselves from known and emerging scams related to COVID-19, including the following:

1. Independently verify the identity of any company, charity, or individual that makes contact regarding COVID-19;
2. Carefully check websites and email addresses offering information, products, or services related to COVID-19 because scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating;
3. Be skeptical of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes, as legitimate health authorities will not contact the public in this manner;
4. Avoid clicking on links or opening email attachments from unknown or unverified sources, which may lead to a virus downloading onto your computer or device;
5. Ensure that anti-malware and anti-virus software on your computer are operating and up to date;
6. Ignore offers for a COVID-19 vaccine, cure, or treatment;
7. Check online reviews of any company offering COVID-19 products or supplies and avoid companies whose customers have complained about not receiving items;
8. Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving any donation;
9. Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. DOJ warns against sending money through any of these channels; and
10. Be cautious of "investment opportunities" tied to COVID-19, especially those based on claims that a small company's products or services can help stop the virus.

For the most up-to-date information on COVID-19, visit the Centers for Disease Control and Prevention (CDC) and WHO websites.

**Strategic Management compliance consultants have over 40 years of experience in providing research, analysis, and program support for privacy and security rule compliance. Call us at (703) 683-9600 or contact us online for a tailored assessment of your organization's particular needs.**