

Beware Fraud in the Wake of COVID-19

Actors are leveraging the spread of COVID-19 to deceive U.S. consumers into making decisions that may expose them to financial and health risk. These actions may represent criminals who seek to profit from the sale of untested or unsafe products, state actors who wish to influence the public's perception of the government's response to the pandemic, or a range of motivations in between. Consumers should be skeptical of advertisements or solicitations from unknown entities.

STAC and WSIC assess that increasing demand for medical supplies will continue as the COVID-19 pandemic progresses. A range of malicious actors, including opportunists, organized crime, and state actors may seek to exploit the situation by attempting to introduce bogus or non-U.S. FDA approved COVID-19 test kits and other related cures or treatments into the U.S. marketplace.

The Department of Justice recommends that Americans to take the following precautionary measures to protect themselves from known and emerging frauds related to COVID-19:

- Independently verify the identity of any company, charity, or individual that contacts you regarding COVID-19.*
- Check the websites and email addresses offering information, products, or services related to COVID-19. Be aware that scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov."*
- Be wary of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the public in this manner.*
- Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device.*
- Make sure the anti-malware and anti-virus software on your computer is operating and up to date.*
- Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if a vaccine becomes available, you will not hear about it for the first time through an email solicitation, online ad, or unsolicited sales pitch.*
- Check online reviews of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.*
- Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving any donation. Remember, an organization may not be legitimate even if it uses words like "CDC" or "government" in its name or has reputable looking seals or logos on its materials. For online resources on donating wisely, visit the Federal Trade Commission (FTC) website.*
- Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail.*
- 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. If you decide to invest, carefully research the investment beforehand. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission (SEC) website, <https://www.sec.gov/>.*

For information about the Department of Justice's efforts to stop COVID-19 fraud, visit www.justice.gov/coronavirus. Additional information about the Consumer Protection Branch and its enforcement efforts may be found at www.justice.gov/civil/consumer-protectionbranch.

In addition, the public is urged to report suspected fraud schemes related to COVID-19 by calling the National Center for Disaster Fraud (NCDF) hotline (1-866-720-5721) or by e-mailing the NCDF at disaster@leo.gov.