COVID-19 Fraud & Scam Alert

Scam artists prey on people's fears related to the Coronavirus (COVID-19). Know the tricks and don't become a victim!

Below are some tips from the Office of Inspector General at the U.S. Department of Health and Human Services, and the U.S. Department of Justice.

- Talk to friends and family.
- Never give any money or personal information to anyone who has reached out to you, unless you know or have verified them.
- Be cautious with your Medicare, Medicaid, or health plan member identification number.
- Don't click on links or open email attachments from someone you don't know or an unverified source. Go directly to trusted agency websites to verify any attempted contact or link before clicking. You could download a virus onto your computer or device. If an email is from someone you know, but feels off or suspicious, don't open it and contact that person another way.
- Make sure the anti-malware and anti-virus software on your computer is operating and up to date.

COVID-19 Vaccine Schemes

Be aware of the following schemes related to COVID vaccines:

- Advertisements or offers for early access to a vaccine upon payment of a deposit or fee.
- Requests asking you to pay out of pocket to obtain the vaccine or to put your name on a COVID-19 vaccine waiting list.
- Offers to undergo additional medical testing or procedures when obtaining a vaccine.
- Marketers offering to sell and/or ship doses of a vaccine, domestically or internationally, in exchange for payment of a deposit or fee.
- Unsolicited emails, telephone calls, or personal contact from someone claiming to be from a medical office, insurance company, or COVID-19 vaccine center requesting personal and/or medical information to determine recipients' eligibility to participate in clinical vaccine trials or obtain the vaccine.
- Claims of FDA approval for a vaccine that cannot be verified.
- Advertisements for vaccines through social media platforms, email, telephone calls, online, or from unsolicited/unknown sources.
- Individuals contacting you in person, by phone, or by email to tell you the government or government officials require you to receive a COVID-19 vaccine.

VRX_21_FWACOVID-19_EGWP_OGB

Medicare & Medicaid Scams

Scammers are offering COVID-19 tests to Medicare and Medicaid beneficiaries in exchange for personal details, including Medicare and Medicaid information. Fraudsters are targeting beneficiaries in a number of ways:

- **Phone Fraud**
  - Medicare members receive phone calls from someone who claims to work with the Centers for Medicare & Medicaid Services (CMS). The callers say because of the person's history with medication, they are eligible for Coronavirus testing. The caller wants to come to the victim's home to drop off the test kit. **Medicare is not calling people.**
  - Criminals are calling pretending to be from a clinic or hospital. They will make up stories about one of your relatives falling sick with COVID-19. The scammers then request payment for their medical treatment, or may ask for additional personal information.
  - Scammers are also using robo-calls to make you buy fake health insurance. They may also ask for your personal information in order to get a free coronavirus test kit. This is all fraud to get your private information.

- **Social Media and Email**
  - Some scammers send emails stating that the World Health Organization is sending free COVID-19 at-home tests and all the individual must do is pay for shipping. **This is not true.**
  - Watch out for fake emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other government agencies. These fake emails offer information, products, or services related to COVID-19. The scammers want you to tap links to malicious websites that will infect and lock your device. Then they might ask for payment to unlock your device.
  - Look carefully at the website addresses and email addresses in these emails. Scammers often use addresses that are only a little bit different from the real thing. For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov."
  - Do not open emails asking you to verify your personal information in order to receive an economic stimulus check from the government. This is another scam.

- **Door-to-door Visits**
    - Fraudsters are targeting seniors with door-to-door visits. The scammer will ask for a Medicare or Medicaid number with the promise of providing a coronavirus testing kit.

The personal information collected can be used to fraudulently bill Federal health care programs and commit medical identity theft. If Medicare or Medicaid denies the claim for an unapproved test, you could be responsible for the cost.

If you think you may have COVID-19, contact a health care provider. Do not go in into a doctor's office, urgent care or emergency room without calling first! They will determine the next steps for testing.

Stimulus Check Scams

Many people across the United Stated have been receiving phone calls, texts or emails asking for personal or financial information to get their federal payment. Some may include links to phony websites that look official. Some may ask for your bank account, PayPal, or other financial information with promises of depositing the money into your account. If you receive these texts or emails, ignore them or delete them. Never click on links because you might download malware onto your computer. **These requests are not legitimate.** Checks are being mailed to eligible people who are not receiving funds through a prepaid debit card or direct deposit into a checking account. Most Americans will receive the funds via direct deposit.

Supplemental Nutrition Assistance Program (SNAP) Scams

Scammers are using the COVID-19 situation to steal personal information from Supplemental Nutrition Assistance Program (SNAP) participants. In one potential scam, a website asked SNAP recipients to enter their personal and bank account information to qualify for COVID-related monetary assistance. If SNAP participants are unsure if a request for information is legitimate, USDA advises they contact their local department of social services.

Social Security Administration Scams

The Social Security Administration is not taking any new actions to reduce, suspend, or delay any benefits during this period, although automated actions may continue. If you receive a communication threatening to suspend or discontinue benefits

because SSA offices are closed, this is **most likely a scam**, and **should be reported to the Inspector General**.

Other Coronavirus Scams

Medical Supply Scams

Fraudsters are setting up fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies related to COVID-19. This includes things like coronavirus testing kits, hand sanitizers, disinfecting wipes and other supplies. Personal Protective Equipment (PPE) is also being counterfeited. This includes N95 respirator masks, goggles, full face shields, protective gowns and gloves. When consumers attempt to purchase supplies, scammers take the money and never provide supplies**.** Do not pay for supplies from distributors that you do not know.

Provider Scams

Scammers are contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment. Do not provide a payment to any doctor or hospital calling you. Hang up. If you believe the caller may have been legitimate, call your friend or family member and ask if they were recently treated, if they're insured, and if they received a bill for their treatment.

Fake Cures and Products

Fraudsters are selling fake cures for COVID-19 online. This includes holy water, vaccines, and unproven treatments for COVID-19.

- Do not pay for a COVID-19 vaccine or cure. Ignore offers or advertisements from anyone selling products that claim to prevent, treat, diagnose or cure COVID-19.

Fake Charities

Criminals can use our desire to help each other by asking for donations for fake charities.

- Before donating, research any company, charity, or individual that contacts you regarding COVID-19. Some organizations use words like "CDC" or "government" in the name to try to look real. Scammers may even copy logos from real companies, or create fake logos that look very professional.
- Don't let anyone rush you into making a donation. Real charities will give you information and take your donation when you're ready.
- Don't send money or payments in cash, by wire transfer, gift card, or through the mail.

For more information on avoiding charity scams, visit the Federal Trade Commission (FTC) website.

Investment Scams

Fraudsters are claiming companies can prevent, detect, or cure COVID-19 and that the stock will go up as a result. These promotions are often called “research reports” and make predictions of a specific “target price” for companies with limited information. Check with a trusted financial advisor and don’t fall for these investment scams!

Report Fraud or Attempted Fraud

You can report COVID-19 scam or attempted fraud without leaving your home using one of these telephone hotlines:

- VibrantRx Fraud Hotline: 1-888-274-1370 (calls can be anonymous; you don’t have to leave your name)
- 1-800-MEDICARE
- 1-877-7SAFERX (1-877-772-3379)

You can also e-mail FWA.VibrantRx@medimpact.com or submit using our VibrantRx online reporting form.

You can also file a complaint online at the FBI Internet Complaint Center for scams related to the Internet (e.g., email, websites and social media.)