December 21, 2020

Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines

The Federal Bureau of Investigation (FBI), Department of Health and Human Services Office of Inspector General (HHS-OIG), and Centers for Medicare & Medicaid Services (CMS) are warning the public about several emerging fraud schemes related to COVID-19 vaccines.

The FBI, HHS-OIG, and CMS have received complaints of scammers using the public's interest in COVID-19 vaccines to obtain personally identifiable information (PII) and money through various schemes. We continue to work diligently with law enforcement partners and the private sector to identify cyber threats and fraud in all forms.

The public should be aware of the following potential indicators of fraudulent activity:

- 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

Tips to avoid COVID-19 vaccine-related fraud:

- Consult your state's health department website for up-to-date information about authorized vaccine distribution channels and only obtaining a vaccine through such channels.
- Check the FDA's website (fda.gov) for current information about vaccine emergency use authorizations.
- Consult your primary care physician before undergoing any vaccination.
- Don't share your personal or health information with anyone other than known and trusted medical professionals.

- Check your medical bills and insurance explanation of benefits (EOBs) for any suspicious claims and promptly reporting any errors to your health insurance provider.
- Follow guidance and recommendations from the U.S. Centers for Disease Control and Prevention (CDC) and other trusted medical professionals.

General online/cyber fraud prevention techniques:

- Verify the spelling of web addresses, websites, and email addresses that look trustworthy but may be imitations of legitimate websites.
- Ensure operating systems and applications are updated to the most current versions.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Do not enable macros on documents downloaded from an email unless necessary and after ensuring the file is not malicious.
- Do not communicate with or open emails, attachments, or links from unknown individuals.
- Never provide personal information of any sort via email; be aware that many emails requesting your personal information may appear to be legitimate.
- Use strong two-factor authentication if possible, using biometrics, hardware tokens, or authentication apps.
- Disable or remove unneeded software applications.

If you believe you have been the victim of a COVID-19 fraud, immediately report it to the FBI (ic3.gov, tips.fbi.gov, or 1-800-CALL-FBI) or HHS OIG (tips.hhs.gov or 1-800-HHS-TIPS).

For accurate and up-to-date information about COVID-19, visit:

- coronavirus.gov
- cdc.gov/coronavirus
- usa.gov/coronavirus
- fbi.gov/coronavirus
- justice.gov/coronavirus
- oig.hhs.gov/coronavirus