Department of Justice

United States Attorney Billy J. Williams
District of Oregon

FOR IMMEDIATE RELEASE
FRIDAY, MAR. 20, 2020
WWW.USDOJ.GOV/USAO/OR

CONTACT: KEVIN SONOFF
PHONE: (503) 727-1185
KEVIN.SONOFF@USDOJ.GOV

U.S. ATTORNEY SHARES TIPS FOR AVOIDING COVID-19 SCAMS TARGETING VULNERABLE POPULATIONS

PORTLAND—Today, U.S. Attorney Billy J. Williams warned of several new fraud schemes seeking to exploit the evolving coronavirus public health emergency by targeting vulnerable populations.

Scammers have already devised numerous methods for defrauding people in connection with COVID-19. They are setting up websites, contacting people by phone and email, and posting disinformation on social media platforms. Some examples of scams linked to COVID-19 include:

- **Testing scams**: Scammers are selling fake at-home test kits or going door-to-door performing fake tests for money.
- **Treatment scams**: Scammers are offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19.
- **Supply scams**: Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.
- **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.
- **Charity scams**: Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19.
- **Phishing scams**: Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails designed to trick recipients into downloading malware or providing personal identifying and financial information.
- **App scams**: Scammers are creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.

- **Investment scams**: Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports," make predictions of a specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.

The U.S. Attorney's Office urges Oregonians to take the following precautionary measures to protect themselves from known and emerging scams:

- 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 general public this way.
- 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 there is a medical breakthrough, you won't hear about it for the first time through an email, 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. 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. Don't send money through any of these channels.
- 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.
- For the most up-to-date information on COVID-19, visit the Centers for Disease Control and Prevention (CDC) and World Health Organization (WHO) websites.

On March 19, 2020, U.S. Attorney Williams announced the appointment of a COVID-19 fraud coordinator to lead investigations into known and suspected occurrences of financial fraud related to the nation's ongoing public health emergency.

If you or someone you know believe you've been the target or victim of an outbreak-related fraud scheme, please contact the FBI's Internet Crime Complaint Center (IC3) by visiting www.IC3.gov. If you or someone you know are in immediate danger, please call 911.

The U.S. Attorney's Office COVID-19 fraud coordinator will be notified of tips submitted via the above reporting method.

# # #