Office of Inspector General
Legal Services Corporation

# The Fraud Corner

**(3/24/2020)**

## COVID-19 Fraud Schemes

As part of its Fraud Corner Series, the Office of Inspector General (OIG) is providing Legal Services Corporation (LSC) grantees with the following information and resources related to Coronavirus/COVID-19 frauds and scams. Consistent with concerns discussed during a recent LSC COVID-19 LSC/grantee conference call, many of these scams could target LSC grantees and their client communities. The purpose of this Fraud Corner is to increase grantee awareness of possible scams and encourages grantees to proactively share information with clients to help prevent them from falling prey to scams.

In a press release issued by G. Zachary Terwilliger, United States Attorney for the Eastern District of Virginia, Terwilliger advised that fraudsters frequently target vulnerable individuals during difficult times. Terwilliger elaborated that scammers have already devised numerous methods for defrauding people in connection with COVID-19. Scammers are setting up websites, contacting people by phone and email, and posting disinformation on social media platforms. The press release cited some examples of scams linked to COVID-19:

- 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 also 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 also 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.

Terwilliger urges everyone, especially those most at risk of serious illness, to avoid these and similar scams by taking the following steps:

- 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.

The Federal Trade Commission has also issued tips for keeping COVID-19 or Coronavirus scammers at bay:

- Don't click on links from sources you don't know. They could download viruses onto your computer or device.
- Hang up on robocalls. Don't press any numbers. Scammers are using illegal robocalls to pitch everything from scam Coronavirus treatments to work-at-home schemes. The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it might lead to more robocalls, instead.
- Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or experts saying they have information about the virus. For the most up-to-date information about the Coronavirus, visit the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO).
- Ignore online offers for vaccinations. There currently are no vaccines, pills, potions, lotions, lozenges or other prescription or over-the-counter products available to treat or cure Coronavirus disease 2019 (COVID-19) — online or in stores.
- Do your homework when it comes to donations, whether through charities or crowdfunding sites. Don't let anyone rush you into donating. If someone wants donations in cash, by gift card, or by wiring money, don't do it.

The LSC OIG urges those who believe they were the victim of a scam to contact their State Attorney General's Office or the appropriate federal, state or local authorities. If you have any questions or comments or would like additional information about this post please contact Daniel O'Rourke, Assistant Inspector General for Investigations at the LSC OIG, (202) 295-1651 or by email dorourke@oig.lsc.gov.