10 TIPS
to Avoid Coronavirus Scams

1. **Watch out for phishing scams.** Phishing scams use fraudulent emails, texts, phone calls and websites to trick users into disclosing private account or login information. Do not click on links, open any attachments or respond to any pop-up screens from sources you are not familiar with. Never give your password, account number or PIN to anyone.

2. **Ignore offers for a COVID-19 vaccine, cure or treatment.** If there is a medical breakthrough, it wouldn't be reported through unsolicited emails or online ads.

3. **Rely on official sources for the most up-to-date information on COVID-19.** Visit the Centers for Disease Control and Prevention, World Health Organization and your state's health department websites to keep track of the latest developments.

4. **Remember that the safest place for your money is in the bank—it's physically secure and it's federally insured.** When you deposit your money at a bank, you get the comfort of knowing that your funds are secure and insured by the government. You don't have the same level of protection when your money is outside the banking system.

5. **Do some research before making a donation.** Be wary of any business, charity or individual requesting COVID-19-related payments or donations in cash, by wire transfer, gift card or through the mail.

6. **Keep your computers and mobile devices up to date.** Having the latest security software, web browser and operating system are the best defenses against viruses, malware and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.

7. **Recognize and avoid bogus website links.** Cybercriminals embed malicious links to download malware onto devices or route users to bogus websites. Hover over suspicious links to view the actual URL that you are being routed to. Fraudulent links are often disguised by simple changes in the URL. For example: www.ABC-Bank.com vs ABC_Bank.com.

8. **Change your security settings to enable multi-factor authentication for accounts that support it.** Multi-factor authentication—or MFA—is a second step to verify who you are, like a text with a code.

9. **Before you make any investments, remember that there is a high potential for fraud right now.** You should be wary of any company claiming the ability to prevent, detect or cure coronavirus. For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission website **www.sec.gov**.

10. **Help others by reporting coronavirus scams.** Visit the FBI's Internet Crime Complaint Center at **www.ic3.gov** to report suspected or confirmed scams. You can also stay up-to-date on the latest scams by visiting the FTC's coronavirus page at **ftc.gov/coronavirus**.