

## Don't Fall for the Scams

In response to the COVID 19 pandemic consumers are encouraged to beware of impostor scams. Impostor scammers will typically call, email, text or direct message consumers on social media, often claiming that Social Security or Medicare benefits are being withheld due to COVID-19, in an attempt to trick victims into clicking on a link or handing over personal information. Please stay vigilant and follow these tips below to avoid scams:



- ❖ **Don't give information or money to anyone who calls, texts, emails, or direct messages you on social media.** Keep your Social Security, bank account, debit and credit card numbers to yourself.
- ❖ **Never make a payment to someone you don't know, especially by gift card, mobile payment apps, money transfer, or cryptocurrency.** Only scammers will demand you pay that way. Scammers know these payments are hard to reverse.
- ❖ **When in doubt, check it out.** If you're concerned about the request, contact the agency directly. Look up the government agency's real phone number on the agency's website and call to get the story.
- ❖ **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 or open any attachments or pop-up screens from sources you are not familiar with, and NEVER give your password, account number or PIN to anyone.
- ❖ **Recognize and avoid bogus website links.** Cyber criminals embed malicious links to download malware onto devices or route users to bogus websites. Hover over suspicious links to view the actual URL where you will be routed.
- ❖ **Report the scam to the FTC at [ReportFraud.ftc.gov](https://www.ftc.gov).** Tell your bank, and be sure to share these tips with your friends and family.

If you have any questions please call our Customer First Contact Center at (203) 462-4400  
(Mon – Fri 8:30 a.m. to 4:30 p.m.)

March 5, 2021