TO ALL MEMBERS:
IMPORTANT INFORMATION ON COVID-19 SCAM TO WATCH OUT FOR

The FBI recently released information on the uptick in COVID-19 scams that they have been seeing lately.

Here are some things you need to know to keep you and your family safe from these scammers:

Fake CDC Emails

Attackers are preying on people by sending emails that claim to be from the Center for Disease Control and Prevention (CDC). Be sure to verify information, such as the "From email address", spelling and other things, to verify the legitimacy of any email, especially those claiming to have information on Covid-19. Don't click on links if anything appears suspicious as they could contain malware or even ransom-ware that will infect your computer. The CDC will not be connecting you by email out of the blue if you have not been in touch with them first.

Stimulus Check Emails

Another type of phishing email being reported is one that asks for verification of personal information in order to receive stimulus checks. Please be aware that the government will not send emails to confirm **ANY Personal Information**. Also be on the lookout for emails claiming to offer charitable contributions, general financial relief, airline carrier refunds, fake cures and vaccines and fake testing kits in response to the pandemic.

False Treatments/Equipment

Fraudsters are capitalizing on people's desires to stay healthy during this time. In turn, they've started scams claiming to sell Coronavirus treatment and prevention products, as well as protective equipment such as face masks, face shields, gloves, sanitizing solutions etc.

What can you do to protect yourself?

- Be aware of the potential schemes that are going around in the wake of COVID-19. Be weary of solicitous emails and phone calls and go into each one of these situations with an air of caution. The following tips will help you as well:
- If you don't recognize the sender, don't open any attachments or click on any links.
- If you don't recognize the phone number, let it go to voice mail and you can then screen the call to see if you even know the caller.
- Personal information which includes your username, social security number, address, phone, birth date should never be disclosed in response to an email or phone call. If your financial institution or legitimate government offices are calling you, they already have that information and would not be asking for it.
- Confirm the website is legitimate by typing the URL directly into your browser (rather than clinking a link). Go straight to the source about COVID-19 at cdc.gov,conroavirus.gov.
- If you receive a phone call get the phone number and financial institution or government office name and then look up that on the internet. Every legitimate office has a phone number that you can call to confirm that they were calling you.
- Check for misspelling, questionable email addresses and bad grammar, as these often signify fraud.

REMEMBER IF YOU RECEIVE AN EMAIL OR PHONE CALL ASKING FOR ANY PERSONALS INFORMATION, THE EMAIL OR CALL IS A PHISHING SCAM AND YOU NEED TO DELETE THE EMAIL OR HANG UP THE PHONE IMMEDIATELY. THE GOVERNMENT KNOWS WHERE TO SEND YOUR STIMULUS CHECK SO THEY WILL NOT BE CALLING YOU FOR YOUR ACCOUNT INFORMATION OR SOCIAL SECURITY NUMBER.

IF IN DOUBT DELETE IT.