SCAMS AND FRAUDS TO WATCH OUT FOR.

The Board of Directors has put together the enclosed information on which SCAMS and Frauds to watch out for as a means to help protect you. The information was obtained from financial institutions, Westchester County, AARP and the DMV. By no means is this a complete list you should always be alert and never release personal information to anyone over the phone, text or emails.

We hope you find the attached information helpful

The Board of Directors

January 4, 2021

Be alert for SCAMS

The following is a list of various SCAMS(received, from Morgan Stanley, AARP or Westchester County) for either Banking, COVID-19, Vaccines. Including SCAMS directed at Seniors for Covid & the Covid Vaccine also for the DMV.

NEVER give out personal information over the phone.

COVID-19 and Vaccine SCAMS:

The Westchester County Department of Consumer Protection is warning all Westchester residents to be vigilant for COVID-19 vaccine scams as we enter the next phase of the pandemic.

Westchester County Executive George Latimer said: "There are vaccine scams out there. People may solicit you, may sound professional and look for money and information from you to get a vaccine. Don't fall for it and don't pay attention to it."

Consumer Protection Director Jim Maisano said: "If you get a call, text, e-mail or even someone knocking on door claiming they can get you early access to the vaccine, hang up, delete or close the door – stop all communication immediately. It's a scam every time."

Tips for Westchester residents based on tricks scammers are using:

- Vaccine is expected to be free.
- There are no sign-up lists for vaccine.
- You can't pay to get your vaccine earlier.
- Medicare or Social Security won't be calling you about getting your vaccine (scammers often act like they are calling from government agencies).
- You don't need to give out SSN, credit card or bank info before you are able to get vaccine.

Maisano added: "Also, beware of scammers or even salespeople offering to sell you unnecessary products, treatments or medicines to prevent the virus - always check with your doctor first. If you are contacted by someone looking to sell you early access to the vaccine, contact Westchester Consumer Protection at (914) 995-2155 or at conpro@westchestergov.com.

Seniors:

Though we've only seen one COVID-19 vaccine scam in SIRS at this point, we know that this this type of fraud will move very quickly, very soon, and will take many forms. Scammers rapidly alter their tactics and adapt their schemes to the changing landscape, and we anticipate that they will leverage the pending COVID-19 vaccine to prey on unsuspecting beneficiaries. At this point, it is essential that we alert the public of likely schemes and provide them with information on how they can protect themselves:

- You likely will not need to pay anything out of pocket to get the vaccine during this public health emergency.
- You cannot pay to put your name on a list to get the vaccine.
- You cannot pay to get early access to the vaccine.

Be alert for SCAMS

- No one from Medicare or the Health Department with contact you.
- No one from a vaccine distribution site or health care payer, like a private insurance company, will call you asking for your Social Security number or your credit card or bank account information to sign you up to get the vaccine.
- Beware of providers offering other products, treatments, or medicines to prevent the virus. Check with your health care provider before paying for or receiving any COVID-19-related treatment.
- If you get a call, text, email — or even someone knocking on your door — claiming they can get you early access to the vaccine, STOP. That's a scam.

As you receive specific vaccine fraud case information, **please notify the SMP Mailbox (smp@acl.hhs.gov) and me (marissa.whitehouse@acl.hhs.gov)** via email ASAP. Additionally, if you have a beneficiary who you believe might be willing to speak about their experience with being approached/contacted about this type of fraud, please email me directly.

We are working closely with the OIG and will provide more information as soon as it becomes available. Please reach out to me with any questions related to COVID-19 vaccine fraud.

Appreciatively,

Marissa Whitehouse
Program Manager, Senior Medicare Patrol
Office of Healthcare Information and Counseling
Administration for Community Living
U.S. Department of Health and Human Services
202-795-7425 | Marissa.Whitehouse@acl.hhs.gov| www.ACL.gov

Beware New Text Message Coronavirus Scams

The latest bunch of text messaging scams targets New Yorkers with phony offers of fake grants, tax refunds, pandemic relief, and unemployment insurance payments — but all the scammers really want is to steal money and personal information from you, warned officials from the New York State Division of Consumer Protection.

"Throughout this public health crisis, scammers have been hard at work preying on unsuspecting New Yorkers," Secretary of State Rossana Rosado said in an announcement Thursday. "This latest batch of scams prey on New Yorkers seeking pandemic relief by spoofing official government agencies."

Scammers are enticing victims to click on links to phony websites. Their messages contain official-sounding phrases such as "pandemic stimulus relief," "Treasury Department," and "government payment" — like this one highlighted by the Orangetown Police Department.

Be alert for SCAMS

Stay Cyber-Safe:

Financial Make sure your money ends up in the right hands with these steps

- Pay with a credit card: Avoid cash or gift cards
- Use secure sites: Ensure the URL begins with https:// ("s" denotes a safer, secure site)
- Take your time: Be wary of urgent requests for money or information

Verify instructions: Verbally confirm with the sender any wire instructions you receive via email

Never give your Social Security Number, password or Debit card pin verbally, email or via text, log into the site remotely.

Charity Scams:

Any such frauds involve faux fundraising for veterans and disaster relief. Scammers know how readily we open our hearts and wallets to those who served and those rebuilding their lives after hurricanes, earthquakes or wildfires. Charity scammers are especially active during the holidays, the biggest giving season of the year.

They also follow the headlines: The coronavirus pandemic has brought a bevy of phony appeals to donate to victims or emergency response efforts.

Sham charities succeed by mimicking the real thing. Like genuine nonprofits, they reach you via telemarketing, direct mail, email and door-to-door solicitations. They create well-designed websites with deceptive names. (Cybersecurity firm DomainTools has flagged more than 100,000 sites with COVID-19-related domains as "high risk" for fraud.) Some operate fully outside the law; others are in fact registered nonprofits but devote little of the money they raise to the programs they promote.

But with a little research and a few precautions, you can help ensure your donations go to organizations that are genuinely serving others, not helping themselves.

- Do check how watchdogs like Charity Navigator, CharityWatch and the Better Business Bureau's Wise Giving Alliance rate an organization before you make a donation, and contact your state's charity regulator to verify that the organization is registered to raise money there.
- Do your own research online. The FTC recommends searching for a charity's name or a cause you want to support (like "animal welfare" or "homeless kids") with terms such as "highly rated charity," "complaints" and "scam."
- Do pay attention to the charity's name and web address. Scammers often mimic the names of familiar, trusted organizations to fool donors.
- Do ask how much of your donation goes to overhead and fundraising. One rule of thumb, used by Wise Giving Alliance, is that at least 65 percent of a charity's total expenses should go directly to serving its mission.

Be alert for SCAMS

- Do keep a record of your donations and regularly review your credit card account to make sure you weren't charged more than you agreed to give or unknowingly signed up for a recurring donation.

Warning Signs:

Pressure to give right now. A legitimate charity will welcome your donation whenever you choose to make it.

A thank-you for a donation you don't recall making. Making you think you've already given to the cause is a common trick unscrupulous fundraisers use to lower your resistance.

- A request for payment by cash, gift card or wire transfer. Those are scammers' favored payment methods because the money is difficult to trace.
- Don't give personal and financial information like your Social Security number, date of birth or bank account number to anyone soliciting a donation. Scammers use that data to steal money and identities.
- Don't make a donation with cash or by gift card or wire transfer. Credit cards and checks are safer.
- Don't click on links in unsolicited email, Facebook or Twitter fundraising messages; they can unleash malware.
- Don't donate by text without confirming the number on the charity's official website.
- Don't assume pleas for help on social media or on crowdfunding sites such as GoFundMe are legitimate, especially in the wake of disasters. The FTC warns that fraudsters use real victims' stories and pictures to con people.

Department of Motor Vehicles (DMV):

DMV make you aware of various text message phishing schemes targeting our customers, and to share tips that you can follow to protect yourself.

These fraudulent text messages are made to look like they are from the NYS DMV and they include a link to a fake DMV website. The messages ask the recipient to update their contact information in an attempt to gain access to sensitive personal data.

If you receive such a text message, you should not provide any personal data and should delete the text right away.

make you aware of various text message phishing schemes targeting our customers, and to share tips that you can follow to protect yourself.

These fraudulent text messages are made to look like they are from the NYS DMV and they include a link to a fake DMV website. The messages ask the recipient to update their contact information in an attempt to gain access to sensitive personal data.

If you receive such a text message, you should not provide any personal data and should delete the text right away.