Below are some alerts, reminders, and other information compiled from various sources that may be helpful for you to use as a reference for developing public awareness sharing with older adults, family members and caregivers in your community – in flyers, agency newsletters, during community presentations or senior programs, radio or TV programs, newspaper articles, etc.

New Social Security Scam:

- Constant and harassing phone calls similar to fake Internal Revenue Service calls from criminals impersonating SSA officials.
- Ability to spoof caller IDs makes it look like a legitimate call from Social Security.
- Sample of demands and threats from scammers: (1) pay for new Medicare card by putting hundreds of dollars on gift cards – there is no charge for the new replacement cards that don't include Social Security numbers anymore; (2) you will lose Social Security benefits unless you provide personal information; (3) scammers impersonating Medicare representatives asking to verify Social Security numbers; (4) your Social Security number has been suspended for suspicious activity; (5) asking for information so you can get a bigger Social Security check; (6) threaten that your benefits will be stopped; (7) Social Security computers are down and they need your help in providing some information; (8) asking to see person's old Medicare card, which shows the Social Security number; (9) pretending to return a call from you regarding Social Security benefits.
- Any suspicious calls that appear to be from the Social Security Administration should be reported immediately to the Office of the Inspector General for Social Security at 800-269-0271 (fraud hotline), or submit a report online at https://oig.ssa.gov/report.

Gift Card Scams:

- Gift card scams are increasing.
- Warning about new and increasingly common scam with callers pretending to represent a federal or state agency. They contact consumers about a fictitious debt and demand payment in the form of a prepaid gift card or risk punishment. Always remember that a government agency will never ask for payment in the form of a prepaid gift card.
- Although many older adults may be reluctant to do so because they don't want to seem impolite, they should be encouraged to simply hang up the phone immediately and report the call to local law enforcement.
- Never read or text someone the PIN number on the back of a gift card. The number is as good as cash in the scammers' pocket.
- Reputable businesses don't ask for gift cards as payment.
- If you're buying gift cards as gifts, make sure to buy them from a reputable and known source.
- Always treat gift cards like cash and protect them as you would your wallet.

Charitable Giving Scams:

- Don't assume that charity recommendations on social media platforms or blogs have already been vetted. Research the charity yourself.
- Find out what percentage of your donation will go to the charity and whether you will be charged any fees for making a donation through a fundraising platform website.
- Check to see if the charity is registered with the NY Attorney General's Charities Bureau.
- Websites posing as charities can sometimes look identical to the real organization. These fraudulent websites will often ask for personal or financial information over an unsecure connection or may download harmful malware into your computer. Look for a padlock symbol or "https" before the web address indicating that it is secure.
- Avoid being pressured to make an immediate donation. Don't hesitate to ask questions to get more information.
- If you didn't initiate contact, avoid giving personal or financial information over the phone. This is an important rule for all phone contacts people receive.
- Never write out a check or give cash to an individual solicitor. Make checks payable to the charity.

Shopping and Computer Related Scams:

- Only shop on secure websites. Look for https in the address (the extra "s" is for "secure") and for a lock symbol.
- Consider paying with a credit card that offers fraud protection when possible.
- Some retailers and delivery services need extra help during seasonal times, but beware of solicitations that require you to share personal information online or pay for a job lead. Apply in person or go to retailers' main stores or websites to find out who is hiring.
- Computer scams
    - Person receives call from someone claiming to be an IT professional saying your computer has a virus. Scammer assures you that the virus can be removed, but scammer needs access to the computer. Scammer then installs software allowing retrieval of anything stored on the computer, recording key strokes, acquiring bank and credit card information and passwords.
    - Pop-up window warning that the computer has a virus and you need to click on the install button to remove it. Clicking on the link can give a scammer access to the computer and any information stored in it.

Chimney Cleaning or Repair Fraud:

- Several of our neighboring states have discovered recent problems with chimney repair scams. As we move further into the winter months you may want to alert older adults and caregivers in your communities about ways to avoid these scams.
- As with any home repair service, beware of suspicious phone calls, door-to-door solicitations, and direct mail offering very low prices for chimney services.
- If repairs are suggested, do not feel pressured by claims of urgent need for immediate work to begin. Disreputable businesses know it is difficult to verify need for chimney repairs and prey on a homeowner's fear.
- Ask for photo or video proof of need for repairs and make sure it has enough background included so you can clearly identify it as your home.
- Broken debris does not necessarily mean repairs are needed. It may not even be from your chimney. Ask them to show you exactly where the pieces came from.
- Before you meet with a service person become familiar with products and repairs specific to fireplaces and chimneys.
- Ask questions.
    - How long has the company been in business?
    - As for current references?
    - Check with the Attorney General's Office and Better Business Bureau regarding any complaints.
    - Does the company maintain professional credentials?
    - Does the company carry the proper insurance?

Some of this information was adapted from November and December 2018 articles from USA Today; Tennessee Department of Commerce & Insurance; New York State Attorney General; The Hickman in West Chester, PA; Better Business Bureau of Central New England; Chimney Safety Institute of America.

December 2018
The Elder Abuse Education and Outreach Program is funded by the Monroe County Office for the Aging and the New York State Office for the Aging