Additional Tips on Preventing and Addressing Financial Exploitation

Adapted from the American Bankers Association
https://www.aba.com/

Older Americans can help protect themselves from financial exploitation by following these tips-

- Keep personal information private. Never share your social security number, account information, or personal details over the phone or internet, unless you initiated contact with a trusted source.
- Shred receipts, bank statements and unused credit card offers before throwing them away so fraudsters can't piece together your personal information.
- Never let a new or untrusted "advisor" pressure you into sharing personal or financial details. They could be a fraudster.
- Check your credit report at least once a year to ensure no new credit cards or accounts have been opened by criminals in your name.

Register your phone number at the Do Not Call Registry to stop solicitation calls. Do not answer phone calls from numbers you don't recognize, instead wait and check your voicemail message.

If you suspect that you or a family member have been the victim of elder financial abuse, take immediate action-

- Victims should report the suspected abuse to the bank and enlist their help in fixing and preventing fraud.
- Victims should contact the local police and Adult Protective Services in the appropriate town or state to report the problem.
- Call the Victim Connect Hotline at 1-855-484-2846 or the Eldercare Locator helpline at 1-800-677-1116.

For more information, visit: https://www.justice.gov/elderjustice/find-supportelder-abuse.

Consumer Tips - Phishing-

- Don't click on suspicious links or attachments. Visiting unsafe, suspicious or fake websites can lead to the intrusion of malware. Be cautious when opening e-mails or attachments you don't recognize even if the message comes from someone in your contact list.
- Never give out your personal financial information in response to an unsolicited phone call, fax or email, no matter how official it may seem.
- Do not respond to email that may warn of dire consequences if you do not validate your information immediately. Contact the company to confirm the email's validity using a telephone number or website you know to be genuine. Clicking on a link could give a criminal access to your personal information.
- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Report discrepancies immediately.
- When submitting financial information on a website, look for the padlock or key icon at the top or bottom of your browser, and make sure the web address begins with "https." This signals that your information is secure during transmission.
- Report suspicious activity to the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center at www.ic3.gov.
- If you believe you have responded to a spoofed email, contact your bank immediately so they can protect your account and your identity.

For additional resources, please see

https://www.aba.com/advocacy/community-programs/safe-banking-for-seniors/safe-banking-for-seniors-consumer-resources