Dear Neighbor:

My office gets many questions regarding scam phone calls, texts, and emails. Scammers often target older adults and try to convince the recipient they owe money or that a relative is in need. These calls are scary, annoying, and for those who believe the calls are real, can be costly.

There is substantial evidence that this is a growing problem. According to the Federal Trade Commission (FTC), complaints about telephone scams jumped from 3,200 in 2017 to 35,000 in 2018 with financial losses rising from $210,000 to $10 million. The Washington Post recently reported that more than 26 billion robocalls were placed to U.S. phone numbers in 2018, up from 18 billion in 2017. Scammers frequently are located overseas and use technology that make calls hard to track, making it extremely difficult for authorities to identify and prosecute them.

This newsletter will offer some general information about types of scams and what to do if you receive a scam call or email. On Tuesday, July 16th I will also be holding a public forum on scams from 6-8pm at Lenox Hill Hospital, Achiles Building, Weisner Conference Room 201A/B, 130 E 77th St, 2nd Floor. For more information on the event, see the item at the end of this newsletter.

Liz

GENERAL RULES FOR AVOIDING SCAMS AND PROTECTING YOUR IDENTITY

- Any caller that asks you to give your Medicare number, Social Security number, mother's maiden name, birthdate, birthplace, username, password, credit card information, billing information, and/or other identifying information is a fraud. Never give your personal information through a phone call, email, mail, or in-person service.
- Do not send money or give credit card or online details until you have checked the credentials of the company that you are dealing with.
- Do not give in to pressure to make a decision immediately. Scammers usually will try to get you to answer or send money right away. Hang up the phone, and do your research before you make a decision to do anything.
- Do not answer calls from unknown numbers. If you do pick up and learn it is a scam call, do not engage. Hang up immediately.
- Do not respond to any questions on the phone, especially those that can be answered with "Yes" or "No".
- Beware of unusual payment methods. Scammers often ask for payment by wire transfers, preloaded cards and even Google Pay, Steam, iTunes cards or Bitcoin. This is nearly always a sign that it is part of a scam. Never send money through a prepaid gift card or card. Government agencies never ask for money from gift cards or prepaid debit cards.
- Do not open suspicious texts, pop-up windows or emails—delete them. If an email appears suspicious, do not open attachments or click on links in the text. If unsure, verify the identity of the contact through an independent source such as a phone book or online search. Don't use the contact details provided in the message sent to you.
- Beware of any requests for your details or money. Never send money or give credit card numbers, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else: money laundering is a criminal offense.
- Choose your passwords carefully. Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower case letters, numbers and symbols. Don't use the same password for every account/profile, and don't share your passwords with anyone.
- Cover or block the Point of Service /ATM keypad when you enter your PIN
- Carry only the identification, checks, credit cards, or debit cards you really need.
- Use direct deposit for paychecks, tax refunds, benefit payments, etc.
- Shred documents with personal/financial information before disposing of/recycling them.
- Review financial statements and bills monthly and identify/correct errors.
- Review your credit report annually and identify/correct errors. Under federal law, each of the nationwide credit reporting agencies — Equifax, Experian, and TransUnion — are required to provide you with a free copy of your credit report, at your request, once every 12 months. You are entitled to an additional free report if a company takes adverse action against you, such as denying your application for credit and you ask for your report within 60 days of receiving notice of the action. Go to www.annualcreditreport.com or call 1-877-322-8228 to obtain your free annual credit reports.

DIFFERENT TYPES OF SCAMS

Social Security Scams

Social Security scam calls try to convince you that someone is using your Social Security card to commit crimes, or that there is a problem with your Social Security account, and to clear your name you need to share private information.

An example of a common Social Security robocall:

"The purpose of this call is regarding an enforcement action executed by the US Treasury against your Social Security number. Ignoring this would be an intentional attempt to avoid initial appearances before the magistrate judge for a federal criminal offense. So before this matter goes to the federal claims courthouse or you get arrested, kindly call us back."

Calls can even "spoof" Social Security's national customer service number as the incoming number on the caller ID. Always be cautious and avoid providing sensitive information such as your Social Security number or bank account information to unknown people over the phone or Internet.

If you receive a call, hang up. Do NOT reveal ANY personal data to a stranger who calls you.

If you wish to file a complaint, report it to the Social Security Administration's Office of the Inspector General at 1-800-269-0271 or https://oig.ssa.gov/report.

Go to www.identitytheft.gov/SSA if you are either worried that you are a victim of identity theft or you want to report identity theft.

Medicare Scams

Scam operators pretending to represent Medicare claim that new benefit cards are being issued, the beneficiary's file must be updated, or that someone is eligible for a free medical device. The scammer may ask for your Medicare number and/or banking information, which is then used for identity theft. Any call that asks you to give your Medicare number, Social Security number, credit card information, and/or billing information is a fraud. Hang up and **do not give your personal information**.

If you have any doubt about someone who calls on behalf of Medicare, hang up and dial (800)-MEDICARE or (800)-633-4227.

IRS Scams

There are a number of variations on this scam which involve claims that the recipient owes taxes to the IRS. You can identify the call as a scam if you remember that the IRS does NOT:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card, or wire transfer. Generally, the IRS will first mail a bill to any taxpayer who owes taxes.
- Threaten to immediately bring in local police or other law-enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving the taxpayer the

opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone.

If you receive a call:
- **Do not give out any information. Hang up immediately.**
- Contact the Treasury Inspector General for Tax Administration to report the call at 800-366-4484 or https://www.treasury.gov/tigta/contact_report_scam.shtml.
- You can also report it to the Federal Trade Commission. Use the FTC Complaint Assistant on FTC.gov. Please add "IRS Telephone Scam" in the notes.

If you think you may owe taxes, call the IRS directly at 800-829-1040.

"One-Ring" Phone Scams

This scam involves your phone ringing once or twice before going silent, with the goal being to get you to call back. These calls may appear to be from somewhere in the U.S., as the first three digits look like U.S. area codes; however, the calls are frequently placed from other countries. If you call back, you may be connected to an international phone number and charged a connection fee as well as hefty per-minute fees. The scammer may also leave a message asking you to call back.

To help avoid this scam:
- Do not answer or return any calls from numbers that you do not recognize.
- Before calling unfamiliar numbers, determine whether the area code is international.
- If you do not make international calls, ask your telephone service provider to block outgoing international calls on your phone.
- Always be cautious, even if you think a phone number is legitimate.

If you are billed for a call you made due to this scam, try speaking with your telephone company to get the charges removed. Charges on your telephone bill will show up as premium services, international calling, or toll-calling. If that does not work, you can file a complaint with the Federal Trade Commission at ftc.gov/complaint or by calling 1-877-FTC-HELP.

Grandparent Scams

Grandparent scams involve a call from someone pretending to be your grandchild or any family member, or a third party claiming that a member of your family is in trouble. The person explains that he is in trouble, with a story that goes something like: *"There's been an accident and I'm ____ (in jail, in the hospital, stuck in a foreign country), and I need your help."*

First, hit the pause button so that you can slow down and do not panic. Think of how to determine if the situation is real. Verify the person's identity by asking questions someone else could not possibly answer. If you receive a phone call of this nature, it is best to hang up and then try to verify the whereabouts of your grandchild/family member by calling his or her cell phone directly or contacting his or her parents.

Another way to know if this is scam is how they want to get the money from you. If it is through a wire transfer service (such as Western Union or MoneyGram), an overnight delivery service or courier (with a check or cash), or a prepaid card or gift card, DO NOT do it! Court systems and hospitals do not accept gift cards as payment. Based on a report submitted to the Federal Trade Commission in 2018, people over 70 reported a median individual loss of $9,000 to people who pretended to be their family or friends.

You can report these scam calls to the FTC at ftc.gov/complaint or by calling 1-877-FTC-HELP.

Immigration Scams

The Department of Homeland Security Office of the Inspector General (DHSOIG) reports that the DHS OIG Hotline phone number is being used as part of a telephone spoofing scam. The scammer pretends to be an employee with US Immigration and alters the caller ID system to make it appear as if the call is coming from the DHS OIG Hotline number (1-800-323-8603). The fraudster demands that the victim verifies personal information through numerous tactics, including claiming that they are victims of identity theft.

It is important to note that DHS OIS NEVER uses a hotline number to make outgoing calls. The number is only used to receive information from the public so do not answer calls from 1-800-323-8603.

If you receive a call claiming to be from the DHS OIG Hotline, do NOT provide personal information.

FBI Spoofing Scam

Fraudsters claim to be FBI agents and call people telling them that they are under investigation for certain federal violations. Victims are told that if they don't pay a fee immediately, they will be arrested. The calls are made by spoofing the local FBI field office phone number.

You can file an online complaint with the FBI's Internet Crime Complaint Center https://www.ic3.gov/default.aspx.

Phishing Call,Text, and Email Scams

Voice phishing scams are when callers impersonate legitimate companies such as Apple, Verizon, or major banks to steal money, passwords, personal and financial information. Another variation involves text messages or emails claiming that your debit card has been used to make a purchase and if you do not recognize the transaction, you need to call their fraud prevention helpline, which is provided. Other times, the messages claim that your password has been compromised and you need to click on a link to reset it.

If you call the number provided in the message, the fraudster will answer the phone and will ask you to confirm your banking information, which will allow them to steal money from your account. Clicking on links in fraudulent texts and emails can enable scammers change your passwords, download malware onto your device, or access personal information.

Do NOT call the phone number provided claiming to be from your bank or other company. If you need to discuss details about your banking account, call the number printed on the back of your debit or credit card or visit a local branch.

You can report these scam calls to the FTC at ftc.gov/complaint or by calling 1-877-FTC-HELP.

Lottery and Sweepstakes Scams

These scams try to trick you into giving money upfront or your personal details in order to receive a prize from a lottery, sweepstake or competition that you never entered. Scammers claim that you need to pay fees or taxes before your 'winnings' or prize can be released. You may also have to call or send a text to a premium rate phone number to claim your prize.

Lottery scams may use the names of real overseas lotteries to claim that you've won cash, even though you never entered into them. Scammers normally ask for fees or taxes to release the funds. They will also tell you they need your personal details to prove you are the correct winner but then use this information to steal your identity or money from your bank account.

Fake vouchers and gift cards involve scammers sending you an email or text message or a social media message claiming you have won a gift card for a well-known retailer but you need to provide some details before you can claim it. This is an attempt to get personal information which can be used for identity theft or to target you with another scam. Offers like these have also been known to deliver ransomware on your device.

Travel prize scams involve scammers claiming you've won a free holiday or airfares. In fact, what you've actually won is the chance to buy accommodation or flight vouchers. These travel vouchers often have hidden fees and conditions, or may be fake and worthless. Similarly, scammers may offer you amazing discounted holiday packages that just don't exist.

Protect yourself:
- Remember: you cannot win money in a lottery or competition unless you entered.
- Competitions and lotteries do not require you to pay a fee to collect winnings—conduct a search online using the exact wording of the offer. It may help confirm that it's a scam.

"Can you hear me?"—Voice signature scam

These are phone scams where the scammer asks "Can you hear me?" They are hoping to get them to say the word "yes" during the conversation that is being recorded. The fraudster will later use the recording of the victim saying yes as a voice signature to authorize unwanted charges on the victim's utility or credit card account.

Immediately hang up the phone. If you think that you already received a call like this, you need to check your bank and credit card statements as well as your telephone statement to see if there are any unauthorized charges.

If you find unauthorized charges, report these charges as unauthorized as soon as possible. You can report these scam calls to the FTC at ftc.gov/complaint or by calling 1-877-FTC-HELP.

Utility Scam

Con artists pose as representatives from your local gas or electric company. They may call or knock on your door, claiming that you have an unpaid balance and that unless you pay immediately (typically via Green Dot Money Pack prepaid cards or your debit card), they will shut off service.

What you should know:

- Utility providers will never come to your door to collect payment.
- Utility companies will not call to ask for your credit card or bank information.
- Do not trust caller ID alone to verify the identity of the caller. Many scammers use spoofing technology to make the caller ID appear with a valid company name and/or phone number.

If you think that there may be a billing issue with your account, do not provide any information to the caller. Instead, hang up and call the phone number listed on your utility bill.

Counterfeit Prescription Drugs Scam

As prices for prescription drugs increase, many people look to the internet to find cheaper prices for their medications. Unfortunately, fraudsters are aware of this and set up websites that advertise cheap prescription drugs which are usually counterfeit. People who unknowingly purchase these counterfeit drugs soon realize they have been duped when the drugs do not provide any relief from their medical condition or even cause additional health problems.

Charity Scam

Scammers take advantage of people seeking to donate to a good cause or find an answer to a health problem. They collect money by pretending to work for a legitimate cause or charity, or a fictitious one they have created. Often scammers will exploit a recent natural disaster or crisis that has been in the news.

Be cautious of any charity or fundraiser that:

- Refuses to provide detailed information about its identity, mission, costs, and how the donation will go to the charity rather than to the caller or the caller's company.
- Does not provide proof that a contribution is tax deductible.
- Uses a sound-alike name that closely resembles that of a better-known reputable organization.
- Thanks you for a pledge you do not remember making.
- Uses high-pressure tactics such as trying to get you to donate immediately, without giving you time to think about it and do your research.
- Uses excessively emotional appeals.
- Asks for donations in cash or asks you to wire money.
- Offers to send a courier or overnight delivery service to collect the donation immediately.
- Guarantees sweepstakes winnings in exchange for a contribution. By law, you never have to give a donation to be eligible to win a sweepstakes.
- Check the Directory of Charity and Nonprofit Organizations, www.guidestar.org/NonprofitDirectory.aspx to see if the charity is on the list of registered charities.

What to Do If You've Been the Victim of Identity Theft:

- For financial-related fraud, **contact the financial institution** or retailer for the compromised account to report the fraud. Ask them to place a hold on your account and issue a replacement debit or credit card.
- **Contact the credit reporting agencies** to place a fraud alert and a security freeze on your accounts: Go to www.identitytheft.gov to create an identity theft report and create a recovery plan.
- Check your credit reports. Go to www.annualcreditreport.com or call 1-877-322-8228 to get your free annual credit reports. If you see any unfamiliar accounts or transactions on your reports, contact the credit reporting agency to dispute the charges and have any unauthorized accounts removed.
- You may choose to file a police report with your local police department.
- In the event of tax identity theft, go to the IRS' website at www.irs.gov and complete IRS Form 14039, Identity Theft Affidavit. Mail or fax the form according to the instructions. Include proof of your identity, like a copy of your Social Security card, driver's license or passport.

REDUCING UNSOLICITED CALLS, MAIL, AND EMAILS

Unsolicited calls are any unwanted calls including illegal and spoofed robocalls as well as any telemarketing calls. Unsolicited mail is unwanted mail such as pre-approved credit card applications.

HOW TO DEAL WITH CALLS

If you're getting illegal sales calls or automated calls, known as robocalls, from scammers, it is best not to pick up the phone and let the calls go to voicemail. If you do pick up a robocall, do not interact with the caller or automated message. Pressing buttons, requesting to be taken off the call list, and talking to a live person likely just leads to more calls.

Block the Calls

Many cell phone and landline providers offer services to block robocalls and/or alert recipients that a call is coming from an anonymous number. These services may be free or require a small monthly fee. There are also free robocall blocking apps that can be installed on cell phones such as TrueCaller, Calls Blacklist, Should I Answer?, Mr. Number, and Hiya.

Spam Alerts

Some cell phone companies provide a "Spam Alerts" feature to your home phone's Caller ID to help you identify robocalls. Your caller ID will show "SPAM?" before caller's name has been identified as a possible unsolicited call. Contact your provider to find out more.

Reduce Telemarketing Calls by Registering with the Federal Government's National Do Not Call Registry

To register your phone number or get information about the registry, visit www.donotcall.gov or call 1-888-382-1222 using the phone number you want to register. You should get fewer telemarketing calls within 31 days of registering your number.

Report the Calls to the Federal Trade Commission

Report the calls to the FTC at www.FTC.gov/complaint where complaints will help drive FTC investigations and cases. The data is shared with law enforcement agencies and will help the agencies monitor trends and initiate investigations.

Report the Calls to the NY Attorney General's Office

If you believe you are the victim of telemarketing fraud, call the consumer hotline for assistance at 1-(800)-771-7755. You can also report the calls to the the Attorney General's Consumer Frauds Bureau using a complaint form at www.ag.ny.gov/complaint-forms.

HOW TO DEAL WITH UNSOLICITED EMAILS

Unsolicited emails are emails that do not contain enough information and ask for money or something of value. They usually have a link.

Phishing Emails

- Never click on a link.
- Never give personal information that includes date of birth, Social Security number.

How to Limit Your Exposure

- When you create accounts and log-ins for other websites, make sure you leave the box which says, "allow us to send updates to your email" UNMARKED unless you want emails from them.
- You can create two email address—one for personal & professional messages and one for shopping, newsletters, coupons, and other services.
- You can use a disposable email address service that forwards messages to your permanent account. If one of the disposable addresses begins to receive spam, you can shut it off without losing your permanent address.
- Try not to display your email address in public such as blog

posts, in chat rooms, on social networking sites, or in online membership directories.

DEALING WITH JUNK MAIL

Unwanted junk mail such as pre-approved credit card applications can be eliminated using the following tips.

Reduce Receiving Mail That You Do Not Want

You can register at the Direct Marketing Association's (DMA) consumer website: www.DMAchoice.org for a processing fee of $2 for a period of ten years. DMAchoice offers consumers a simple, step-by-step process that enables them to decide what mail they do and do not want.

If you do not wish to complete your registration online, you can register by using the mail-in form that is online which is found at https://dmachoice.thedma.org/static/pdf/registration_form.pdf. Or if you do not have access to the Internet, you can register by sending your name, your address, and your signature, along with a $3 processing fee (check or money order payable to DMA) to:

DMAChoice
DMA
PO Box 900
Cos Cob, CT 06807

If you decide that you do not want to receive prescreened offers of credit and insurance, you can opt out of receiving them for five years or opt out of receiving them permanently.

- To opt out for five years: Call toll-free 1-888-567-8688 or visit www.optoutprescreen.com
- To opt out permanently, you can visit www.optoutprescreen.com and return the signed Permanent Opt-Out Election form, which will be provided after you initiate your online request.

If you don't have access to the Internet, you may send a written request to permanently opt out to each of the major consumer reporting companies. Make sure you include your home telephone number, name, Social Security number, and date of birth.

Experian
Opt Out
PO Box 919
Allen, TX 75013

TransUnion
Name Removal Option
PO Box 740123
Woodlyn, PA 19094

Equifax, Inc.
Options
PO Box 740123
Atlanta, GA 30374

Innovis Consumer Assistance
PO Box 495
Pittsburgh, PA 15230

Forum on Scams
Tuesday, July 16th, 6 -8 pm
Lenox Hill Hospital, Achiles Bldg., 130 E 77th St.
2nd Floor, Weisner Conference Room 201A/B

This event will include two NYPD officers and Chuck Bell, Programs Director of Consumers Union. The police officers will present a PowerPoint presentation on certain phone scams, unsolicited calls, and email/mail scams, do's and don'ts, and who you can alert when you encounter these scams. Chuck Bell will speak about state and federal government legislative efforts, as well as industry efforts, to protect consumers from these scams.

To RSVP, email lkrueger@nysenate.gov with subject Scams Forum, or call 212-490-9535.

New York State Senate, Albany, NY 12247

State Senator Liz Krueger's
Guide to Dealing with Scams

PRSRT-STD
U.S. POSTAGE
PAID
NEW YORK SENATE

Albany Office:
416 State Capitol
Albany, NY 12247
(518) 455-2297

District Office:
211 East 43rd Street
Suite 1201
New York, NY 10017
(212) 490-9535

E-Mail: lkrueger@nysenate.gov
Website: krueger.nysenate.gov

Resource Guide

Bureau of Consumer Financial Protection (BCFP)
www.consumerfinance.gov 1-855-411-2372

Handles consumer complaints about financial products and services including mortgages, money transfers, debt collection, credit cards, prepaid cards, bank accounts and services, vehicle and other consumer loans, payday loans, student loans, credit reporting, and virtual currency. Complaints can be submitted online at www.consumerfinance.gov/complaint or by calling 1-855-411-2372.

The Office for Older Americans is a special office within the BCFP's Division of Consumer Education and Engagement dedicated to helping Americans age 62 and older make sound financial decisions.

Federal Trade Commission (FTC)
www.ftc.gov 1-877-FTC-HELP (382-4357)
www.ftc.gov/idtheft 1-877-IDTHEFT (438-4338)

The Federal Trade Commission FTC website offers practical information on a variety of consumer topics. The www.Identitytheft.gov website offers information on what to do if you are the victim of identity theft.

National Center on Elder Abuse
www.ncea.acl.gov/

The Administration for Community Living sponsored website provides resources on elder abuse prevention, including information on reporting a suspected case of elder abuse.

Financial Industry Regulatory Authority
www.finra.org 1-800-289-9999 (BrokerCheck Hotline)

Find out about the broker's background via the brokercheck.finra.org. Or call the FINRA BrokerCheck Hotline. Find out more about the use of senior designations or certifications at finra.org/investors

OnGuardOnline.gov
www.onguardonline.gov

The federal government's website to help you be safe, secure and responsible online. The FTC manages the site in partnership with 16 other federal agencies. Its resources include information on phishing available at onguardonline.gov/articles/0003-phishing.

Financial Fraud Enforcement Task Force (FFETF)
www.stopfraud.gov/protect-yourself.html

This is a task force composed of government agencies that has a website with resources on Elder Fraud.

AARP Foundation ElderWatch
www.aarp.org/aarp-foundation/our-work/income/elderwatch/report-fraud/
1-800-222-4444, option 2

AARP Foundation ElderWatch engages hundreds of volunteers each year to help older consumers recognize, refuse, and report fraud and scams. This website provides additional information and tools to help protect consumers against financial exploitation.