Dear Neighbor:

My office regularly hears from constituents with questions and concerns about scam calls, emails, and messages. Scams have unfortunately become increasingly pervasive and sophisticated, and technological advances have made many scams harder to recognize. They can be scary, frustrating, and for anyone who has fallen victim, financially and emotionally costly.

It is important to understand that many scammers are skilled at what they do, and anyone can be a victim. There are scams designed to target people regardless of age, income, profession, educational achievement, or tech savviness. While law enforcement agencies at all levels of government are working to investigate and prosecute scammers, the vast number and variety make this extremely difficult, especially since many scammers are located overseas and/or use advanced technology to hide their identities.

One of the best ways to protect ourselves is to become familiar with the primary tactics employed by scammers so we're less vulnerable. This newsletter is designed to help you minimize your risk of identity theft and other scams, recognize some of the most common scams, and know what steps to take if you are contacted by a scammer. On Thursday, November 14th I will also be holding a virtual public forum on scams from 6:30pm-8pm. For more information about the event, please see the item on the last page.

As always, if you have any questions or need assistance, email or call my office at lkrueger@nysenate.gov or 212-490-9535. If you would like to receive regular email updates from me, please send an email with the subject line "Join Liz List" to lkrueger@nysenate.gov.

HOW TO MINIMIZE THE RISK OF IDENTITY THEFT

- Be extremely cautious whenever anyone asks you for sensitive information such as your address, mother's maiden name, birthdate, Social Security number, or bank information.
- Use direct deposit for paychecks, tax refunds, benefit payments, etc.
- Shred documents with personal/financial information before disposing of them.
- Review financial statements and bills regularly and notify the bank or business if you see any purchase that you didn't make. Some scammers who have your personal information will make small charges first to see if they can get away with it.
- Keep an eye on your mail. Mail theft is one way that identity thieves can gain access to your information. If you are out of town, consider having your mail held at the post office or renting a post office box.
- Review your credit reports regularly to identify and correct any errors. Visit www.annualcreditreport.com or call 877-322-8228 to obtain free credit reports from the major credit reporting agencies.
- If you think your personal information may have been compromised, place a security freeze on your credit reports to prevent any new credit accounts from being opened in your name.

TIPS TO PROTECT YOUR IDENTITY ON ELECTRONIC DEVICES

- Create strong passwords for all your accounts, change them frequently, do not reuse them, and do not share them with anyone.
- Use two-factor authentication to prevent hackers from accessing your online accounts. This is particularly important for accounts that contain your identity and/or financial information.
- Be wary of connecting to public WiFi networks. Remember that even if a network requires a password, it may not be secure. If you use public WiFi often, consider a virtual private network.
- Keep your devices locked and password-protected and ensure that antivirus and security software is on and kept updated. Activate firewalls and other settings that block malicious files.
- Only download free software from reputable sites. Scammers often try to trick people into downloading viruses or spyware by bundling it with free software.
- Avoid clicking on pop-up windows or ads if you don't know the source, even if they are telling you that your computer is at risk. These often contain spyware or malware that can harm your computer and/or give a scammer access to your device.
- Sign out of apps and websites that contain personal and/or financial information as soon as you're done using them.
- Don't overshare on social media. Use privacy controls so information like your birth date, your employer, friends, and family members aren't publicly accessible.
- Do not hand your phone to anyone you don't know. Scammers can access your information or transfer money to themselves while pretending to make a quick call or helping you to make a purchase. If you want to assist someone who asks to make an emergency call, dial yourself and put the phone on speaker.

RED FLAGS OF A SCAM

Although the variety of scams can seem endless, there are some common characteristics that can help you recognize them and avoid being a victim. Be on the lookout for these red flags:

- Any unsolicited outreach via phone, text, email, or social media. Fraudsters often do their research and may already have some personal information about you, so don't let your guard down if someone mentions names of people you know, companies you do business with, their badge number, or claims they work for the government.
- Requests for personal information, or requests to confirm if information is accurate, from anyone who contacts you unsolicited.
- A sense of urgency to act immediately. Scammers prey on emotion and want you to make decisions without having time to think or verify what you're being told. Legitimate companies and government staff will not pressure you to act quickly.
- Scare tactics such as telling you a loved one is in danger or sick, an account is at risk, a new bank account has been opened in your name, or threatening legal action.
- Spelling or grammatical errors in written communication or any use of vulgar or threatening language.
- Requests for payment in a specific way—especially by gift cards, wire transfers, cash, payment apps such Venmo, Cash App, or Zelle, or cryptocurrency.
- Instructions not to share what you're being told or what you should say to others.
- Reasons why you should communicate only with the person who contacted you, or someone they connect you to.
- Instructions to move your money into another account to protect it.
- Limited-time special discounts, loans, prizes, or investment opportunities that you must send money or provide personal information to obtain.

TIPS TO PROTECT YOURSELF FROM SCAMS

- Understand that most scammers engage in "spoofing"—disguising an email address, sender name, phone number, or website URL or using technology to manipulate the name appearing on caller ID—to convince you that you are interacting with a government agency, bank, or well-known company. AI technology even makes it possible for scammers to spoof the voices and images of people you know.

- Government agencies will never contact you unsolicited by phone, email, text, or social media. If you receive a call or message like this, it's a scam.
- Never provide your private information in response to an unsolicited call, email, or text message.
- Do not answer calls from unknown numbers. If it is important, the caller will leave a message. If you pick up a suspicious call, hang up immediately. Do not worry about being rude.
- Block unwanted calls, text messages, and emails. Most phones and email programs have spam filters that make this easier, but fraudsters often find ways around these systems.
- If you are uncertain whether a caller or message you receive is legitimate, do not engage. Contact the person, government agency, or business directly through another means. Make sure to locate legitimate contact information for the entity, such as the number on the back of your bank card or information listed on the institution's website.
- Do not trust unsolicited emails or text messages even if they look legitimate. Many scammers use the logos or letterhead of companies and government agencies to try to appear trustworthy.
- Any time you receive an email from a business, carefully check the sender's address. An email address that doesn't match the company's website domain (i.e. JohnSmith@gmail.com rather than JohnSmith@companyname.com) is a scam.
- Only use peer-to-peer payment apps like Zelle, Venmo, and Paypal with trusted parties. Payments made through these platforms generally cannot be reversed and are frequently used by scammers.

WHAT TO DO IF YOU WERE SCAMMED

- Immediately cut off all communication with the scammer.
- Try not to blame yourself and seek support if needed.
- Notify your bank and credit card companies if you think any accounts may be at risk.
- Check your recent credit and debit card transactions and ask to have any fraudulent charges reversed. Federal law limits consumers' liability for unauthorized charges made with credit and debit cards when cardholders quickly report the fraud to their financial institutions. Visit https://consumer.ftc.gov/articles/lost-or-stolen-credit-atm-and-debit-cards for details.
- Change any usernames or passwords that may have been compromised.
- Document the scam. Gather evidence of fraudulent transactions and communication, and any information that might possibly help to identify the perpetrators.
- If you are concerned that your identity may have been stolen, or if someone is already improperly using your personal information, visit www.identitytheft.gov. This Federal Trade Commission website can help you develop a recovery plan based on the specific situation and file an identity theft report if needed.
- Contact the three credit reporting bureaus and place a security freeze on your credit reports if you think your identity may have been compromised:
    - Equifax: https://www.equifax.com/personal/credit-report-services/credit-freeze/ or 888-378-4329
    - Experian: https://www.experian.com/freeze/center.html or 888-397-3742
    - Transunion: https://www.transunion.com/credit-freeze or 800-916-8800

  A security freeze prevents creditors from accessing your credit report to open a new credit card or loan in your name. If you want to apply for a new credit card or loan in the future, you will need to contact the credit reporting agencies again to temporarily or permanently unfreeze your credit.
- Closely monitor your financial accounts and credit reports going forward and dispute any fraudulent activity. Go to www.annualcreditreport.com or call 877-322-8228 to get your free credit reports and report any errors.
- If you would like more guidance or need support, contact AARP's Fraud Watch Helpline at 877-908-3360 or one of the other organizations listed in the *Resources* section.
- Report the scam. See below for details.

WHERE TO REPORT SCAMS

While law enforcement and government agencies can't always identify and prosecute scammers, they can utilize the information gathered to record patterns of abuse. This may lead to larger investigations and enforcement actions against individuals and networks. Having records of the report(s) may also help you limit damage. Depending on the nature of the scam (or attempted scam), it should be reported to one or more of the following:

- **Local law enforcement:** While all scams can be reported to the police, this is especially encouraged if you lost money or property, had your identity compromised, or are being threatened by a scammer.
- **Federal Trade Commission:** All types of scams and fraud should be reported at https://reportfraud.ftc.gov/ or by calling 1-877-FTC-HELP (1-877-382-4357).
- **FBI Internet Crime Complaint Center:** All cybercrime and scams that take place on the internet should be reported to https://www.ic3.gov/.
- **Social Security, Medicare, and IRS scams** should also be reported to specific government entities. See the *Government Agency Impostor Scams* section for details.

COMMON SCAMS

While there are countless scams and new ones pop up all the time, all scammers are either trying to convince you to give them money and/or your personal information. Below, you'll find an overview of some of the most frequent scams.

BANK IMPOSTER SCAMS

These scams involve a scammer pretending to work for your bank or another financial institution. The scammer may alert you to suspicious activity on your account and tell you that to correct it you'll need to provide personal information, send a payment, move your money to another account, or send them a special code through a payment app. The scammer might also claim that they work for a bank where you don't have an account to alert you that someone has opened an account in your name.

If you receive an unsolicited phone call or message from someone purporting to be from a bank, hang up immediately or move the message to spam. If the call or message was from a bank where you have an account, call the number on the back of your bank card or statement, or visit a local branch, to make certain your account has not been compromised. Never share sensitive information with anyone who calls you out of the blue—even if the name and number on your caller ID belongs to your bank and/or the caller claims to work for fraud protection. If you provided personal information to someone impersonating a bank staffer before realizing it was a scam, carefully monitor yor financial accounts and consider placing a security freeze on your credit reports.

FAMILY EMERGENCY SCAMS

These scams involve calls or emails from someone pretending to be your family member or friend who is facing an emergency, or a third party claiming to be contacting you on behalf of a loved one. They are trying to prey on your emotions by inventing a crisis that you must respond to immediately – with your money. They may use technology to have a familiar phone number appear on your caller ID and reference information available on the internet about you or the family member to make the call seem real. They may even use artificial intelligence to create a voice recording that sounds exactly like your loved one. The person may also try to stop you from confirming their story by begging you not to tell anyone since they are embarrassed or scared.

If you receive a call or message like this, slow down and think about how to determine if the situation is real. To confirm the person is who they say, consider asking specific personal questions that only your loved one would know and would be difficult to find out from the internet or social media. Or even better, hang up the phone and call another relative or even the person who claims to be in trouble

to confirm the story. Another way to know if this is a scam is how they want to get the money from you. If it is through a wire transfer service, payment app, an overnight delivery service, or a prepaid card or gift card, it's a scam.

GOVERNMENT AGENCY IMPOSTOR SCAMS

Government imposter scams typically involve a scammer contacting you via phone, email, text message, or social media claiming to be from a government agency–especially the Social Security Administration, FBI, IRS, Medicare, or Department of Homeland Security. They will likely provide some reason why you need to send money or give them your personal information immediately. These scammers frequently use intimidation tactics, such as threatening legal action or the suspension of benefits, to coerce you to comply. They may urge you not to tell anyone else what is happening and/or demand payment in a specific way. Or the scammer may already have information about you that they claim they need to verify or update.

In order to appear authentic, these scammers may use the name of an actual government employee, give you their employee ID or badge number, or send a message or letter on what appears to be official government letterhead. Calls and messages may come from spoofed numbers that appear to be coming from a phone number associated with the agency; the name of the agency may also pop up on your caller ID.

Government agencies will never call, email, text, or message you on social media unsolicited asking for money or personal information. Only a scammer will do that. You will receive a letter in the mail if there is an actual problem or reason an agency needs to be in contact. If you have any questions about whether a call or message you receive from a government agency is legitimate, it is always best to hang up or ignore the message and contact the agency using the information you find on their website.

If you are contacted by one of these scammers, hang up, block the number, and/or move the message to spam. In addition to the places listed under *Where Should Scams Be Reported*, certain government impersonation scams should be reported to the following:

- **Social Security scams:** Social Security Administration's Office of the Inspector General at 800-269-0271 or https://secure.ssa.gov/ipff/home.
- **Medicare scams:** Medicare helpline at 800-633-4227. The New York Senior Medicare Patrol (800-333-4374) can also help Medicare recipients prevent, detect, and report Medicare fraud.
- **IRS scams:** Treasury Inspector General for Tax Administration at 800-366-4484 or https://www.tigta.gov/reportcrime-misconduct. You should also forward emails to phishing@irs.gov.

SWEEPSTAKES SCAMS

Many scammers attempt to use your excitement to get you to make a bad decision. You may get a telephone call, email, or letter telling you that you've won the lottery or urging you to apply for a sweepstakes because you're already a finalist. The most common ploy is for the scammer to tell you that taxes or fees need to be paid on the winnings so that the prize can be released. You may also be told that your personal details are needed to confirm that you are the correct winner. Other scammers will send messages via email, text, or social media claiming that you have won a gift card for a well-known retailer, but you need to provide some details to claim it.

Legitimate competitions and lotteries do not require you to pay a fee or buy merchandise to collect winnings. And remember that you cannot win any type of competition that you didn't enter. Never send money or provide personal or financial information to anyone who contacts you unsolicited saying you have won any type of prize. Also, avoid clicking on any sort of unsolicited message claiming that you have won a competition—it may contain malware or spyware.

PACKAGE DELIVERY SCAMS

You've likely received one if not many of these text messages stating that your post office, UPS, or FedEx delivery has been put on hold because of a problem with your address, insufficient postage, or nobody was home. The messages usually ask you to click on a link to provide more information, pay for extra postage, or reschedule delivery. The link will likely take you to a legitimate-looking website often with the logo of the delivery service and an actual tracking number, where you are asked to verify your address, and perhaps pay a small "redelivery fee."

These messages are almost all from scammers trying to steal your money and/or identity—do not click on any of the links and send them to your spam folder. If you're concerned that there might be a problem with a package you're expecting to receive or have sent, contact the service directly, not through the link.

PHISHING SCAMS

Phishing scams usually use spoofing techniques to convince you to share valuable personal and financial data, such as your Social Security number, credit card details or passwords for online accounts, and to steal your identity, your money or both. These scams primarily occur via email but come in many forms including via social media messages, phone, text message, and drawing victims to bogus websites.

In a typical phishing scam, you might receive an official-looking email from a bank, utility, internet provider, or a well-known company like Amazon or Netflix, claiming that there's a problem with your account that needs to be fixed by clicking on a link or calling a customer service number. The message may claim that you are being offered a special discount, your password has been compromised, you need to verify a purchase was made with your credit card, or say that you need to update your personal information. But if you click on the link provided, you'll be sent to a spoofed website that looks nearly identical to the real thing and asked to enter sensitive personal and financial information. These fake websites are used solely to steal your information and/or your money. Clicking on links in many of these messages can also enable scammers to change your passwords, download malware onto your device, or access personal information. If you call the number provided, you'll be connected to a scammer.

If you receive any sort of unsolicited message or phone call stating that there is a problem with your account or asking for your personal information—do not click on the link or provide any information. Legitimate companies will not contact you this way asking for personal information. To check whether a business or government agency is really trying to contact you, use its legitimate customer-service email or hotline, which you can find online or on account statements. Forward phishing emails to the Federal Trade Commission at reportphishing@apwg.org and then designate the message as spam in your email or phone.

TECH SUPPORT SCAMS

These scams come in a variety of forms and have been growing exponentially in recent years. In one common variation, you receive a call, email, text, or pop-up message from a scammer who claims to have found a problem with your computer that can be fixed if you allow remote access to your computer. Other times, you might receive a pop-up message informing you that you have a virus or an error on your computer that can only be fixed by clicking on a link or calling a phone number and they can fix it before you lose all your data.

Don't believe any of these calls or messages, click on any links, or give remote access – legitimate tech support companies will never contact you unsolicited. If you receive one of these messages or pop-ups on an electronic device, it's best to close your internet browser, restart your device, or even manually press the "off" button if needed to get rid of a fake virus-warning pop-up. If you are concerned that your computer may have been infected, run an antivirus program and consider contacting a reputable source for help. Be careful though when searching for businesses on

the internet – sometimes scammers place ads for illegitimate tech support services online.

VOICEPRINT SCAMS

In an older version of this scam, a fraudster will call and ask: "Can you hear me?" They are hoping to get you to say the word "yes" during the conversation, which is being recorded. A recording of the victim saying yes can be used as a voice signature to authorize unwanted charges on the victim's utility or credit card account. With recent technological advances, it's now possible for thieves to capture a recording of your voice from videos posted to social media, your voicemail message, or by calling and recording your voice and then use a software program to generate an imitation "deepfake" version that can be used to impersonate you. That voiceprint can be used to try to access your financial or insurance records, transfer money out of your accounts, or carry out a scam against your loved ones.

The best way to prevent your voice from being recorded and/or duplicated is to avoid all calls from unknown numbers. If you pick up the phone and realize the call is suspicious, immediately hang up and do not worry about being rude. If you think that you have already received a call like this, carefully monitor your financial accounts and immediately report any suspicious activity.

WORK FROM HOME SCAMS

As remote jobs have become more common, the number of scams offering work from home jobs has grown exponentially. You might receive an email, text message, or call promising that you can make thousands of dollars a month working from home, or simply asking if you are interested in remote work. Some scammers also pose as legitimate businesses such as staffing agencies. If you respond, you will likely be told that you need to pay for training, products you will supposedly sell, or to "unlock" the job opportunity—all these payments will go directly to a scammer. The messages may also include links to websites designed to steal your personal and/or financial information or to add malware to your device. Send all unsolicited job offer messages you receive like this to spam, do not click on any links they contain, and block the sender.

Senator Krueger's Virtual Town Hall on Scams:

Thursday, November 14, 6:30 pm – 8 pm

Jeanine Launay, Elder Abuse Unit Chief, Manhattan DA's Office
Anthony Nuccio, Detective, 19th Precinct Crime Prevention
Kathleen Benedetti-Fisher, Scam Expert, AARP New York

To RSVP, please email lkrueger@nysenate.gov with "Scam Town Hall" in the subject line or call 212-490-9535.

New York State Senate, Albany, NY 12247

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

State Senator Liz Krueger's
Guide to Dealing with Scams

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

District Office:
211 East 43rd Street
Suite 2000
New York, NY 10017
(212) 490-9535

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

RESOURCE GUIDE

AARP Fraud Watch Network

https://www.aarp.org/money/scams-fraud/
Fraud Watch Helpline: 877-908-3360

AARP's Fraud Watch Network helps people of all ages proactively learn how to recognize, avoid, and report scams, and offers free confidential support groups for victims and their loved ones. Their Helpline provides personalized guidance, support, and referrals for victims of scams and their loved ones. You do not need to be member of AARP or a minimum age to receive assistance from their Fraud Watch Helpline.

Federal Trade Commission

https://reportfraud.ftc.gov/ 877-FTC-HELP (382-4357)
https://www.identitytheft.gov/ 877-IDTHEFT (438-4338)

The Federal Trade Commission (FTC) offers in-depth information on how to identify, avoid, and respond to scams and fraudulent business practices of all types. Visit https://reportfraud.ftc.gov/ to report a scam and get practical advice on the steps you can take to protect yourself. The FTC's website https://www.identitytheft.gov is the federal government's one-stop resource for identity theft victims.

National Elder Fraud Helpline

833-FRAUD-11 (833-372-9311)

The U.S. Department of Justice's National Elder Fraud Hotline is staffed by experienced case managers who provide personalized support to adults ages 60 and older who are victims of scams and other forms of financial fraud. Case managers can assist with identifying appropriate reporting agencies, filing complaint forms, and referrals to other support services as needed.

NYPD Scam Information Hotline

646-610-SCAM (7226)

The NYPD's 24-hour hotline provides guidance, information, and resources to New Yorkers who are victims of scams or potential scams.