



HOW TO FIGHT BACK

Tips for Seniors on Avoiding Scams

Brought to you by –

Attorney General William
Tong, State Reps. Liz
Linehan, Jack Fazzino, and
State Senator Jan
Hochadel

Table of Contents

Chapter	Page
1. Why are Scammers so Successful?	3
2. Common Scams	4
3. A Few Tips to Stay Safe	19
4. What to Do When Scammed	23
5. About Wiring Money	24
6. Preparing for a Medical Emergency	25
7. OAG Elder Abuse Hotline	26
8. Contact Information	27

Welcome!

Dear friends and neighbors,

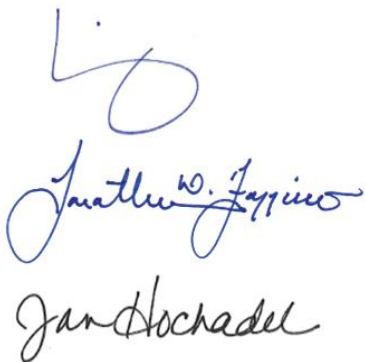
Thank you for coming to our event this morning. It's an honor for us to serve Cheshire in the legislature, and a great pleasure to bring our constituents real-life solutions staying safe and avoiding scams.

There will be a great deal of information given to you today, and we've compiled this booklet for you to take home and continue to have the information at your fingertips when you need it. We understand that seniors are more likely to experience scams, which is why we remain committed to working on solutions that will provide resources and assistance to equip you against scammers.

From enacting legislation, to strengthening support for elders, we want to show you various options to keep seniors safe and aware of potential scams that happen much too often. By providing full transparency on common scams, you'll know what to do when scammed, and have a few tips to stay safe.

We hope you find this information both informative and applicable. Please feel free to share your thoughts with us, and if you need help assistance with contacting the Elder Abuse Hotline listed in this packet, please do not hesitate to contact us directly.

Warm regards,

Three handwritten signatures in blue ink. The first signature is 'Liz', the second is 'Jonathan W. Fazzino', and the third is 'Jan Hochadel'.

Liz Linehan, Jack Fazzino, and Jan Hochadel

Why are Scammers so Successful?

Why are many scammers successful?

The techniques used by scammers usually feed on **fear and bullying, built on emotion**. If you receive an unsettling call, whereby you are told a loved one is in trouble or you owe money, your emotions are triggered, and many times fear takes over. Once this happens, common-sense and logic disappear. This is what the scammers count on and what it makes it much easier to scam someone because they are now making decisions based on emotion. **The other technique that makes scammers successful is that they do not do it face-to-face. It is much harder to deceive someone if you are face-to-face with them, than over the phone.**

Let's talk about common traits of scammers. They:

1. contact you out of the blue and unsolicited
2. give a sense of urgency
3. ask you for personal information
4. tell you to keep it a secret and not tell anyone
5. try to befriend you
6. become angry and may use profanity if you resist
7. will threaten you if you do not comply. The FBI will not give you a heads-up that they will be coming to your house to arrest you, nor will they arrest you over \$500
8. communicate in broken English and/or with bad grammar
8. ask you for money or to send them gift cards--gift cards are for gifts—not payment



It is very common for scammers to direct the consumers to purchase gift cards from local stores and put hundreds of dollars on these cards. The scammers then ask for the identification numbers on the backs of the cards. Once this is done, the scammers activate the cards and remove the money. The consumer is out of their money and there is no way to locate the scammers. **Never purchase gift cards for someone that you don't know.**

Common Scams

Why are so many seniors are scammed out of money and personal information? Many are getting ready to retire and have saved for it, tend to have fewer large expenses (mortgages are paid off or they have downsized to smaller houses with less operating expenses or small mortgages). Some seniors may be very susceptible because many are home during the day or live alone, have time on their hands, would welcome someone to talk to. Below is a list of the most common scams we see today. Please note that new scams are popping up every day, but the more you know, the easier to spot someone trying to swindle you!

1. The Unsolicited Phone Calls

- Our offices receive many complaints from consumers receiving unsolicited phone calls. Consumers call our office with the phone number of the caller and want us to put a stop to these calls. Unfortunately, it's not that easy because most scam calls are from "spoofed" numbers. This makes it look like the caller is calling from a certain phone number, when in fact they are not. These calls are not traceable. They are trying to scam money from you, so they are not too concerned about the laws, or breaking them including the Do Not Call list.
- **Best advice from sources:** use a robocall blocking device.
 - You can try one, such as DCB plus (For about \$50, it imports all phone numbers from your contact list, and only calls from those on your contact list go through)
 - Nomorobo
 - YouMail, a totally free robocall blocking app and call protection service for mobile phones. YouMail blocks unwanted robocallers by making sure the user's phone doesn't ring, and then plays an out-of-service message that leads them to think they dialed an invalid number, and more.
 - Contact your mobile carrier, as some of them offer free robocalling apps.

Scammers are good at what they do. They are going to be nice and convincing. If not, you would not want to talk to them or fall for what they say, and they would be out of business. Don't be tempted. If they call you, **HANG UP THE PHONE.**

- **Do not:**

- Respond to any phone calls, e-mails or mail that are unsolicited and appear suspicious in nature
- Trust caller ID – It can be and is often spoofed. If you want to call to verify any information you've been given, look up the website or telephone number yourself rather than clicking on a link or calling the customer service number provided. Their number may lead you right back to scammers.
- "Press a number to not receive any more phone calls from them", as pressing this number confirms your # is active and scammers can then use your phone # to make scam calls

- **Do:**

- Google the phone number via the internet to see if it is from the company the person is representing themselves to be from or to see if anyone else has reported complaints about the call or phone number
 - Ask the caller for their phone number so you can call them back
 - Report these calls to the FTC. They track them and sometimes are able to locate the callers and, in some cases, prosecute them
 - Consider purchasing a call-blocker (DCB Plus or nomorobo or YouMail). Go to FTC's website for more info
 - Contact your wireless carrier for options on blocking these calls. Some are free.
- **Legitimate calls** coming into your home have to be made between 8 a.m. and 9 p.m. The solicitor must provide his name and the name, phone number and address of the company they are calling from. They are required to immediately comply with any do-not-call request you make during the call.
 - **Debt collectors** or those portraying to be debt-collectors cannot use profanity, threaten violence, arrest or deportation, or harass you to pay. They cannot lie or pretend to be someone they are not nor ask you to pay a debt that does not exist. Nor can they tell anyone about your debt, except your spouse or your attorney.
 - **Our own Attorney General, William Tong**, joined 51 other Attorney Generals and 12 companies **against illegal robocalls**. Phone companies will work to prevent illegal robocalls by:

- Implementing call-blocking technology at the network level at no cost to customers
- Making available to customers additional, free, easy-to-use call blocking and labeling tools
- Implementing technology to authenticate that callers are coming from a valid source
- Monitoring their networks for robocall traffic

Phone companies will assist attorneys' general anti-robocall enforcement by:

- Knowing who their customers are so scammers can be identified and investigated
- Investigating and taking action against suspicious callers – including notifying law enforcement and state attorneys general
- Working with law enforcement, including state attorneys general, to trace the origins of illegal robocalls
- Requiring telephone companies with which they contract to cooperate in traceback identification

2. Romance Scams

- Romance scams are at their highest level in 2023¹
- Most losses occurred through bank transfers, then gift cards²
- Gift card romance scams increased by a staggering 70% in 2020³
- Not surprisingly, this scam affected older people the most
- Nearly 70,000 people reported losing \$1.3 billion in romance schemes in 2022⁴
- These scammers pay close attention to the information people share to become your perfect match. However, they make excuses for not being able to meet in real life, such as they are out of the country on a military base or working on an “offshore oil rig”. The scammers common lies include:
 - I or someone close to me is sick, hurt or in jail
 - I can teach you how to invest
 - I’m in the military far away
 - I need help with an important delivery
 - We’ve never met but let’s talk about marriage
 - I’ve come into some money or gold
 - I’m on an oil rig or ship

¹ National Council on Identity Theft Protection: 2023 Identity Theft Facts and Statistics, pg. 1

² National Council on Identity Theft Protection: 2023 Identity Theft Facts and Statistics, pg. 1

³ National Council on Identity Theft Protection: 2023 Identity Theft Facts and Statistics, pg. 1

⁴ Federal Trade Commission: Consumer Protection Data Spotlight: Romance scammers’ favorite lies exposed by Emma Fletcher, February 9, 2023

- I need money for a visa to come be with you in the States
- You can trust me with your private pictures—however, once you send the pictures, the scammer then threatens to share them on social media unless you send them money (sextortion) ⁵
- Scammers often use dating apps and start with an unexpected message on social media
 - Scammers may begin their first contact on a legitimate dating site, but then quickly ask you to move to a private chat, such as Google Hangout, because it is not monitored.
- Ways to spot a romance scammer:
 - Nobody legitimate will ask you to help by sending them cryptocurrency or gift cards or send money to receive a package
 - Try a reverse image of their profile picture to see if they align with the information they provided⁶

Here's the bottom line:

Never send money or gifts to a sweetheart you haven't met in person!

3. The “Emergency”/ Grandparent Scam

These involve calls from a family member needing money, and are often during an “emergency”. Imagine this scenario: Your phone rings, and a young woman says, “Nana, I got into an accident, and they won’t let me leave without paying them for their bumper! They said they’d call the police, because I don’t have my license. Don’t tell my mom, please Nana, I’m scared they’re going to hurt me!” Reading this, you think you won’t fall for it, but even the best and brightest do – because they prey on your emotions, and because they are very good at what they do. And they’re getting better at it, too. The FTC now reports that these scams are using artificial intelligence. All these scammers need is access to your family member’s social media, and a clip of their voice. The computer does the rest, and you are led to believe it’s really your granddaughter, *because it sounds just like her.*

- If you get this or a similar call, and if someone else is with you, **have them call the phone number** of the loved one the scammer is purporting to be.

⁵ Federal Trade Commission: Consumer Protection Data Spotlight: Romance scammers’ favorite lies exposed by Emma Fletcher, February 9, 2023

⁶ Federal Trade Commission: Consumer Protection Data Spotlight: Romance scammers’ favorite lies exposed by Emma Fletcher, February 9, 2023

- **ask for the phone number of the caller** and tell them you will call them back. This will allow you time to call the real number of the loved one, or give you time to **google** the phone number to see if others are receiving such calls.
- **Call the police.** The scammer will make you believe your loved one is essentially being held for ransom, and involving the police will get them killed. **This is a red flag.**
- **Try to stay calm.** Remember, scammers move fast and prey on your emotions. Try to stay calm and level-headed to make good decisions. Practicing this scenario will help you make the right choices if you are targeted.
- **PRE-PLAN: Talk to your kids and grandkids about a code word or phrase to use when they're really in trouble.** Tell them never to share this phrase, and use something easy to remember. Re-iterate it often. If you're forgetful, leave it on a post it near the phone in your home. If you get this call, ask what the code word is. You'll know it's a scam when the person doesn't know it.

4. Identity Theft

- Identity theft is when a person gains access to your personal information and misuses it for their own gain—usually a financial gain.
- **Do:**
 - Report it to **IdentityTheft.gov** which is a federal government reporting site and provides you with a checklist as to what you have to do
 - Call one of the 3 credit reporting bureaus, Equifax, Experian, and TransUnion, so they can put a **fraud alert** on your credit report
 - Fraud alert: businesses must try to verify your identity before extending new credit. This is usually done via a company calling you to ask if you are really trying to open a new account. As of 9/1/18, these alerts will last for a full year. It is free.
 - Complete a complaint form at ftc.gov/complaint. This will create an identity theft affidavit which assists you in creating a police report
 - Consider putting a "security or credit freeze" on your credit file at these reporting bureaus
 - This will freeze everyone out of your credit file, even yourself

- It prevents anyone and everyone, including yourself, from opening new lines of credit, unless additional, personal information is provided. You'll get a PIN number to use each time you want to freeze and unfreeze your account to apply for new credit. To lift the freeze, you have to contact each reporting bureau. As of 9/21/18, these freezes are free.
- Frank Abignale recommends Privacy Guard as a credit monitoring company.
- Order a free copy of your credit report from each of the three reporting bureaus once a year, so you can check on the accounts to ensure you are the one that opened them
- Contact your Homeowner carrier as some policies provide certain coverage for identity theft

5. The "Can You Hear Me Now" Scam

- This is when you receive a call and the person fumbles around, makes an excuse such as she is adjusting her headset, then asks "Can you hear me now?" When you respond "yes," the scammers record this response, then use it later as a way of confirming you signed up for a particular product or service.

6. IRS Scam/Debt-Collector/FBI Scam

- **Tax-related identity** theft is a common form of identity theft. Consumers received calls from people purportedly being from the IRS, FBI, Collections, etc. They threaten to have someone come to your house for payment. None of these organizations will call to forewarn that someone is coming to arrest you for a few hundred dollars or threaten you. If you owe money, they will send you a letter.
- Remember that by law, debt-collectors cannot call you before 8 a.m. or after 9 p.m., use profanity, threaten violence, lie, or pretend to be someone they are not
- Calls from scammers purporting to be from the IRS are a common scam these days. File your taxes as early as you can. If you receive such a call, you should:
 - Alert your accountant
 - If you owe Federal taxes, or think you might owe taxes, hang up and call the IRS at 800-829-1040. IRS workers can help you with your payment questions.

- If you do not owe taxes, fill out the "IRS Impersonation scam" form on TIGTA's (Treasury Inspector General for Tax Administration) website, www.tigta.gov, or call TIGTA at 800-366-4484.
- You can also file a complaint with the Federal Trade Commission at www.FTC.gov. Add "IRS Telephone Scam" to the comments in your complaint.

7. The Jury Duty Scam

- The caller portrays to be calling about a jury duty obligation that you missed. If you provide him with certain personal information—such as DOB or Social Security Number or bank account #--he offers to take care of it, so your name is not turned over to the proper authorities. Do not provide the caller with any information.

8. The Live-in Companion Scam

- You hire someone, "Sally," from an agency to be a live-in to assist a family member. Sally passes all employment background checks. Sally then hires others, unbeknownst to the live-in agency or family members, who goes and lives with the elder person. Sally gets a cut of the money the family is paying for the live-in helper even though she is not taking care of your family member.
- If you hire a live-in companion for yourself or a loved one, purchase nanny cams. Alert the worker you have them in your home, and that they are monitored by family members to lessen the risk of theft or physical or mental abuse.

9. Purchasing a Car

- **Do Not:**
 - Purchase a vehicle over the internet that you have not actually seen or test-driven
- **Do:**
 - Review the maintenance logs of the vehicle. These will give you an idea as to whether the car was taken care of or neglected.
 - Ladies should bring a man or mechanic with them. Perception can be everything. There is a lesser chance of being taken advantage of or buying a car with issues. (Note from Representative Linehan: This is sexist, but

unfortunately true. Don't be afraid to question out loud if they are taking advantage of you. Require mechanic to write down all tests and their results, along with suggested repairs and costs, and tell them you'll get a second opinion. Don't be afraid to speak up if you feel they are trying to swindle you, trust your gut and speak up!)

- Take the vehicle for a test drive before you sign any documents. Many complaints come from when the buyer does not even get the vehicle home before it breaks down.
- Lift the floor mats—is the carpeting wet or smell like mildew? Are there water lines on the panels? **These are signs that the car endured a flood.**
- Obtain a Carfax report before the actual purchase
- There is no cancellation provision on purchases
- There is no 3-day right of rescission
- There is no Lemon Law protection for used cars—only for new cars
- If a warranty exists, it will be stated on the Purchase Agreement

10. Internet

- Just like we use the computer and internet more than ever, so do the scammers
- When receiving an email asking for personal information, including passwords, click on the email header and look for the senders address. The name may read “Amazon”, but upon further inspection, it's a yahoo or AOL address (for example), and not from Amazon.
- If you receive a link to pay a bill in an email, don't pay it through that link. Go directly to the website before you enter any username or password. This is actually best practice for any unsolicited email
- Again, it is much easier to scam someone when not face to face. Scammers will pose as a buyer for an item you are selling.
- **Do not:**
 - Respond to unknown requests from a company or person thru the internet. If it is a company, look up the number yourself and call the company directly.
 - If you receive an unwanted e-mail and can “Click here to remove your e-mail address from further communications,” DO NOT CLICK ON IT. This will

simply confirm your e-mail address to those sending the e-mail. Use a “mark as spam” filter if your email service has one.

- Click on a link in an e-mail. Re-type the link in the address bar.
- **Facebook Marketplace** is popular with scammers. When selling something on Facebook, the seller will often be asked by a potential “buyer” to confirm they are a legitimate seller by giving your cell number to the buyer, who then texts you a code. They ask you for that code as a way to "prove you are real." However, that text code allows the scammer to open a Google Voice account in your name, allowing them to scam others with a Google Voice phone number associated with you. Never agree to supply a code to anyone.

11. Texting Scams

- These scams typically involve a bank stating there is a problem with your credit card. It gives a phone number to call and then prompts you to enter your credit card number. Or it could be Amazon, Netflix, Hulu, or something you may use often saying your account has been compromised, and you need to change your password. They say that to get your password and steal your information. **These companies will not text you a link to change your password or billing information.**
- **Do Not:**
 - Reply to these messages by hitting the “Stop” button at the end of the message. All it does is confirm to the scammers that your phone number is active.
 - Click any links in the text
- **Do:**
 - If you feel there is a problem with your credit card or bank, look up and call the customer service phone number and speak directly with a representative
 - If you do reply to the scam text, contact your bank or credit card company ASAP
 - Call your cell phone provider and block the number from where the text originated

- When you receive a spam text message, forward the text to 7726 (which spells spam). Your cell phone provider will ask you for the spam phone number. The spam number will be recorded into a database for possible action to be taken against them.

12. Lottery Scam

- You cannot win if you don't play. And you cannot win if you do not buy a ticket. Ignore the letters you receive stating you have won when you know you have not purchased a ticket. Despite how enticing it is, **NEVER** respond to a letter congratulating you on winning, but in order to cover the taxes or costs of sending you the prize money, you need to send money. Legitimate contests do not have you pay to claim your prize.
- Lotteries from out of the country are illegal

13. Delivery companies (especially around the holidays)

- One tactic involves thieves following a parcel delivery truck along its route. Once the package is delivered and the coast is clear, they steal it to look for electronics and other valuables. Sometimes criminals will walk around a neighborhood looking for packages left on people's property.
- The other prevalent delivery scam involves emails with a subject line such as "Missed Delivery Notification." They look like they come from a legitimate delivery company or retailer, and are designed to make you believe that the email is a legitimate call to action to claim the parcel.
The phony emails claim a company was unable to deliver a package to you, and urges you to click on a link to supposedly track the shipment or arrange another delivery by opening an attachment in the email. You also may be redirected to an authentic-looking website and asked to enter personal or financial information. Either action can download malware onto your computer to steal personal information.
- **Legitimate delivery companies will leave a tag on your door** if nobody was home to accept a parcel. They will not send you an email.

- **Ignore email notices about missed deliveries** - Now that you know about the fake "missed delivery" emails, be wary of them regardless of where they appear to come from
- **Arrange for pickup** - If you are expecting a delivery and not able to wait for it, let the driver know you will pick up the parcel yourself by making that selection on the delivery tag
- **Ask for delivery at a specific time** - You also can select an option for the parcel to be delivered at a given date and time when you know you will be home. You also can track a package, and if it doesn't show up, call to see if it was delivered.
- When you order merchandise for delivery, have it shipped to your workplace or a neighbor to prevent its theft

14. Home Improvements

- **Do Not:**
 - Pay for repairs up-front. Stay away from those that require this. Usually, it is okay to give a deposit, but not full payment. Another option is for the Contractor to tell you specifically what materials are needed and you can purchase them for him. Then, you will only owe for labor, which does not get paid until the Contractor has actually done work.
- **Do:**
 - Try to use a Contractor who has worked for people you know and comes recommended
 - Make sure the contractor is registered with the Dept. of Consumer Protection. You can go online to the DCP website of www.elicense.ct.gov or call 800-842-2649 and check to see.
 - Obtain the contractor's Certificate of Insurance prior to any work being done. Make sure it is current and covers the time period that the work will be done - protection if you have to make a claim against him or he gets hurt on the job. Don't listen to any excuses from the Contractor as to why he cannot provide you with a copy. It is as easy as him calling his insurance agent.
 - Get more than 1 estimate. This will ensure that the cost for the work you are having done is competitive.

- Ignore the urgent, hard-sell, limited-time offers
- Check with your local building officials to verify if permits are required and whose responsibility it is to pull these permits
- There is a Guaranty Fund through the Department of Consumer Protection. It allows you to access funds if the contractor is registered and you obtain a judgment against him in court for not complying with the terms of the contract for faulty work. Contact your State Representative or Senator for help filing a complaint.
- Home improvement contracts must include:
 - 3-day notice of cancellation that allows consumers to cancel within 3 days
 - details on how to cancel
 - a valid phone and fax # of the contractor and his mailing address. When you decide on a contractor, get a signed contract.

15. Work From Home Opportunities or Mystery Shoppers

- **Do not:**
 - Accept an offer where you are asked to go shopping at a store, such as Walmart, and then rate the Customer Service. You are asked to cash the check you were sent by the “employer,” keep a certain amount as your pay, then wire the balance through Western Union or Money Gram. The check you were told to deposit will bounce and you will lose the money you wired.
 - Discuss how they operate and show them the fake checks and how you are asked to send a portion of the check you received by cutting a check out of your own account via Money Gram or Western Union to a P.O. Box. The check you receive may look like any other check from a business, contain the name of the business you know and the name of a known bank with a routing number. But go to cash it and you will find out it is a fake. Has anyone received a check like this?
 - When in doubt, call the bank where the check is drawn and ask them if this is their routing number and address. (it may be – but the account number will be wrong)
 - Pay to work a job

- Invest in a starter kit or buy materials ahead of time
- There are very few legitimate ones. Just as you are seeking an income, so are they. Fraudsters are especially active during tough economic times. They know the more desperate a person is, the more they let their guard down and are most vulnerable.
 - Discuss phishing—when a scammer puts out an ad from a legitimate business, but with a different P.O. Box than that of the legitimate business. The scammer is trying to obtain a person's private identifying information (S.S.#, DOB, phone number, address, etc.). This later leads to identity theft.
- Newspapers and websites are putting warnings into their Help Wanted sections, alerting consumers about some bogus work opportunities

16. Foreclosure Rescue

- Be very wary of companies contacting you with an offer to assist you with lowering your mortgage. There are some legitimate companies out there, but most are not. They are targeting the people who can least afford to lose money yet are the most desperate. Easy prey for the scammers. Again, **never pay up-front fees**. These mortgage reduction companies must be licensed. Also, there is a fee cap of \$500.
- It's **illegal** for a business to ask you to pay for mortgage relief services until you've received an offer from the lender and accepted it

17. Tech Support Scams

The 'tech support scam' works like this:

- A person receives a call at home from someone who claims to be a 'tech support specialist' with a well-known computer or software company.
- The caller says that your computer has been infected by a malicious virus or spyware. He may use scare tactics, claiming that your computer will crash or the information on it will be misappropriated if you don't immediately fix the problem.
- The caller says he can correct the problem for a fee if you allow him to remotely install anti-virus software, usually by going to a website to which he sends you.

- Wanting your computer to be fixed, you visit the website and give him your credit card number.
- Weeks later, you may discover that your account was charged not only for the supposed software repair 'service,' but also for other unauthorized transactions.
- If you let the caller install a program onto your computer by visiting his website, you may also find that malware or spyware has been installed on your computer that allows the fraudster to drain from your computer private bank account numbers.

DO NOT:

- Don't believe the caller. No one from Microsoft, Apple, MacAfee, or any tech company will ever call you to say they know what's on your computer. They don't.
- Don't give them your email
- Don't click any link that comes up saying you're infected!

DO:

- Just hang up the phone and/or close the computer window.

18. The Front Door/Back Door Scam

You receive a knock at the front door, and a very nice person starts a long spiel, hoping you will sign a petition to save the whales, or something to keep you engaged. Meanwhile, their partner is headed around back to sneak in and steal your valuables while you are engaged in conversation.

- **DO NOT**

- engage in conversation without first asking for ID and the company name.
- keep any doors unlocked if you are home alone
- open the door unless you know the person

- **REMEMBER:**

- **Cheshire Police Department** requires all door-to-door solicitors to obtain a permit. Ask to see the permit, along with company ID
- **Political door-knocking teams** come around before every election. This is not soliciting, so a permit is not required. However, legitimate candidates have pre-printed literature about the candidate and the office, and do not solicit donations at the door.
- **Utilities** do not come to your home and ask to come inside without any prior appointment.
- **Call the Police if you are uneasy! They want you to call, and you are not being a bother!**

A Few Tips to Stay Safe

Tips for You and Your Family to be Safer

- Do not carry your Social Security or Medicare card on you. Medicare no longer has your Social Security number as your ID. It is too easy for thieves to steal this from you and gain your vital, personal information.
- Use a black or blue uniball gel pen, as this ink cannot be altered
- After reconciling your credit card and bank statements for accuracy, shred your personal information, instead of throwing it in the trash. Get a micro-cut shredder that cross-shreds the documents into tiny pieces, instead of long strips that can be taped back together.
- When possible, pay by credit card. If you have an issue with a charge or a purchase, you have a certain amount of time in which you can dispute this with your credit card company. They will investigate and reverse the charges if they feel the transaction is not legitimate. The fewer, the better on the number of credit cards you have.
- Mail: Do not put your bill payments in your mailbox! Putting up the red flag is an alert to scammers that there is mail in there. Drop your mail INSIDE at the POST OFFICE if you are paying by check.
- Retrieve your mail from your box ASAP.
- Check your credit regularly. You can get 1 free credit report per year. The FTC recommends www.annualcreditreport.com.
- Practice safe computing:
 - When you are using a public computer, avoid conducting business or banking transactions - especially if you are using free public Wi-Fi that doesn't require a password
 - Update software and malware protection to protect your computer from corrupt malware

- When selecting security questions, do not select those where the answer is public information and can be easily obtained by the scammers, such as your mother's maiden name or city where you were born
- Do not store passwords on your computer. Make strong passwords and change them on a regular basis
- Keep your computer antivirus protection up to date.
- ATM and GAS STATIONS: watch out for skimmers. They are card readers that go over a real card reader to steal the information when you swipe your card. They are cheap, fast, and easy to install, but hard to notice. When entering your PIN, block yourself from those behind you and make sure no one is standing behind you as they can take a video with their phone of you entering your PIN.
- When possible, use Apple Pay or touch pay pads.
- File your income tax returns early, to reduce your chances of someone else filing them in your name with your personal information.
- Keep in mind that law enforcement (police, FBI, IRS, court) will NEVER call you on the phone and ask for money or personal information. Nor will they give you a heads-up that someone will be there shortly to arrest you.
- Be aware of yourself and others: has someone recently tried to befriend you or a friend or elderly person? Has this person tried to isolate this elderly person from family and friends? Has an elderly person recently made an unexpected change to their will/financial accounts or in conservatorship? THESE ARE **RED FLAGS** that this elderly person may be being coerced to do so by someone trying to scam them.
- Never send money to someone you do not personally know.
- Do not send money using Western Union or Money Gram unless you personally know the recipient. There is very little, if anything, our office or law enforcement can do to track these scammers down and retrieve your money. Once your money is sent, it is gone. You will receive a confirmation # when you send money. You can then track it over the internet to see if the money has been picked up, but that is about all that you can learn about it.
- Do not deposit a check into an account and send an unknown someone a portion of it from your own account.

- Know the difference between cash available in your account and when a check has cleared:
 - Cash available—does NOT mean the check has cleared. If you access these funds before the check has cleared, the bank will want their money back from you if the check bounces.
 - Check has cleared: the funds are in your account for your use
Many times, when you receive a check, you can deposit it when you receive it. By law, the banks must make deposited funds available within a few days, but it may take up to 2 weeks or so for the bank to know if the funds are available and whether it is legitimate, i.e. the check has cleared.
- Do not give personal information such as Social Security Number or password over the internet or phone. Call the company directly. Most companies will ask you for part of your S.S. # or DOB, but not the whole number. That can still be risky. Google the phone number to see if others are receiving the same such calls.
- If you are communicating with someone by e-mail or written correspondence, check for common red flags—poor grammar, misspellings, spacing mistakes, excessive capitalization, use of generic email addresses, rather than specific business e-mail addresses. These red flags are common with scammers.
- Be cautious when dealing with people that state that they are out of the country or live overseas. This would give the scammers a reason not to meet you in person. Likewise, be weary of those that only want to communicate via written correspondence. It is much easier to defraud/lie to someone when you are not face-to-face.
- If someone sends you a friend request on Facebook and you are already friends with them, do not accept this new friend request. Chances are, they have been hacked and the hacker is sending you this request. The same applies with an e-mail that you receive from a friend that tells you to visit a link and the message only contains the link.
- Since 2002, copiers have hard-drives in them. Get rid of the hard-drive in your copier before you get rid of your copier, as thieves buy old copiers and use the information on the hard-drives. Copiers will have records of everything you have copied, scanned, or e-mailed by the machine.

- **Secure important paperwork** - Arrange for sensitive documents to be sent to a permanent address such as your parents' home or your work.
- Do your own homework before dealing with someone you do not know.
- Register all of your phones (home and cell) on the National Do Not Call Registry. 1-888-382-1222 or www.donotcall.gov.
- When in doubt, call or go onto the website of the **Department of Consumer Protection** to see if the business is registered. Registration is not required for all businesses. Check under e-license.
- If dealing with a business in CT, you can go to the **Secretary of State's website** and check to see if the business is registered. Their website is www.concord-sots.ct.gov/CONCORD/Search Database/Business
- Use your gut and look for red flags. If someone was to come to you and repeat the sales pitch you were given, what would you tell this person? Follow your same advice. If the offer sounds too good, it probably is.
- Keep in mind this 3-step approach to minimizing your risk: **Prevention** (do not provide personal information to those you do not know), **Detection** (be alert to suspicious activity), **Resolution** (report any problems or violations to the proper authorities immediately).
- Be proactive: sign up for scam alerts at ftc.gov/subscribe.
- Go to AARP Fraud Network @ aarp.org/fraudwatchnetwork
- Call 211 from your phone or visit www.211ct.org from a computer for a list of various programs and services in CT. This site has 40,000 programs and services and 4000 agencies affiliated with it, from food pantry locations to statistics on issues in CT.

What to do When Scammed

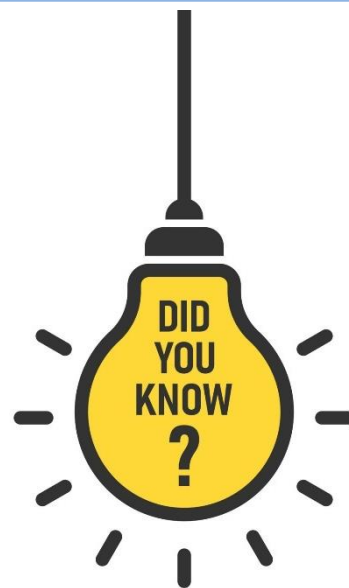
What to do if You Are Scammed

- **Act quickly! If you are scammed, call the Attorney General's office immediately at 860-808-5400 to report it. They have contacts at major companies and may be able to intervene and prevent or lessen your loss.**
- If you suspect identity theft, act quickly. Report it to the Federal Trade Commission. Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or go online: ftc.gov/complaint. The FTC operator will give you the next steps to take.
- Visit ftc.gov/idtheft to learn more. Use IdentityTheft.gov, which will walk you through a recovery plan to make sure you do everything necessary.
- If you send a Western Union Money Transfer® and believe you may be a victim of fraud, call the Western Union Fraud Hotline number at (800) 448-1492. Information on fraud scams is available on the Consumer Protection section of Western Union website at: <http://www.westernunion.com/stopfraud>.
- If you sent money via MoneyGram and believe you are a victim of fraud, call their Customer Care Center at 1-800-926-9400 or go onto their website of www.moneygram.com.
- Additional information on money transfer scams is available from the Federal Trade Commission at: www.ftc.gov.

About Wiring Money

Did you know?

MoneyGram and Western Union Kiosks will warn you about common scams as you attempt to send money. You will see pop-up windows which warn of IRS and telemarketer scams. However, not all scams are listed in these warnings, and not everyone pays attention to pop up windows, either.



Never Wire Money to Anyone Who:

- who you haven't met in person
- who says they work at a government agency like the IRS, SSA, or a well-known company
- who pressures you into paying immediately
- who says a wire transfer is the only way you can pay

Also don't wire money to someone who tries to sell you something over the phone. Not only will you not have the same protections you would paying with a credit card, but it's illegal for a telemarketer to ask you to pay with a wire transfer, like those with MoneyGram and Western Union. Report them to the Attorney General if they ask you to pay this way.

The Top 3 Countries where wire transfers obtained by scam are:

1. Nigeria
2. India
3. China

What To Do If You Wired Money to a Scammer

- Call the CT Attorney General at 860-808-5400 for help
- If you sent money using a wire transfer company like MoneyGram or Western Union, contact that company right away. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

Preparing for a Medical Emergency

Preparing for a Medical Emergency

In case you become ill or have an accident, you should have the following information posted on your refrigerator (or even in a glass jar or jar with identifying label on it in your refrigerator as this is where first responders will look for any medications you may be on) and in your wallet/purse for emergency personnel:

- Name and phone of person to call and their relationship to you
- Name of the hospital you want to go to for treatment
- Name and phone of your primary care provider
- Name of your health insurance carrier and policy number
- A copy of your Health Care Directive, explaining your wishes
- A list of the medications you are currently taking and for what condition are you taking them

Have a document listing the following and assign a trusted person who knows the location of this document and has copy of it:

- The name and phone of your conservator/executor and their relationship to you (a POA is executed in advance of incapacity; a Conservatorship happens upon petition to the court after an individual is no longer able to competently make important financial decisions).
- The name and phone of your attorney, financial advisor and accountant
- Your bank name and account numbers
- Safety deposit box and key location and what documents are in box
- The location of your Will and Health Care Directive, birth certificate and SS card
- A listing and location of your health, life and home/car insurance policy carriers and policy numbers
- Information on your mortgage and any other loans or accounts-- name of company, account number, phone number.
- Have a contact person listed in your phone under ICE (In Case of Emergency)

The Elder Abuse Hotline

The Elder Abuse Hotline

The Attorney General's Office, in cooperation with the Coalition for Elder Justice in Connecticut (CEJC), has launched the Elder Justice Hotline – **1-860-808-5555**, a new resource to help older adults in Connecticut seek information, assistance, and justice.

Have you been the victim of a fraud? Received a message demanding immediate payment and aren't sure if it's legitimate? Have you or your loved one been the victim of abuse or neglect? Do you need help accessing benefits or assistance? If so, our staff can connect you to agencies who are available to help.

The hotline will be staffed by the Attorney General's Office Monday through Friday from 8am to 5pm. If you are calling after hours, please leave a message and your call will be returned as soon as possible.

Recognizing the importance of collaboration, the Attorney General's Office has partnered with the CEJC to provide the Elder Justice Hotline as an additional resource for Connecticut's older residents, their families, and caregivers. The Elder Justice Hotline can successfully connect consumers to the right agency to lodge a complaint, get more information, or get connected to the resources they need.

The Elder Justice Hotline is intended as an additional resource offered to connect individuals seeking information to the appropriate state agencies. The Elder Justice Hotline does not investigate reports of elder abuse, neglect or exploitation. Reports of suspected abuse, neglect, or exploitation received through the Hotline will be referred to the Department of Social Service, Elderly Protective Services Unit. Individuals may also report such complaints directly by calling 1-888-385-4225 (during regular business hours) or to Infoline at 211 after hours, weekend and state holidays. If calling from outside Connecticut, call Infoline at 211 or call 1-800-203-1234. Additional information on how to report elder abuse can be found at Social Work Services--Related Resources (ct.gov)

Contact Information

Name	Contact
Representative Liz Linehan	Liz.Linehan@cga.ct.gov
Representative Jack Fazzino	Jack.Fazzino@cga.ct.gov
Senator Jan Hochadel	Jan.Hochadel@cga.ct.gov
Attorney General William Tong	Attorney.General@ct.gov