

Savvy Seniors: How to Avoid Financial Scams



APRIL 2019

Disclaimer:

For your convenience, this Guide includes hyperlinks to external Internet sites that are not provided or maintained by the Attorney General's Office (AGO). Please note that the AGO cannot guarantee the accuracy, relevance, timeliness, or completeness of these external sites. In addition, the inclusion of links to other sites is not intended to endorse any views expressed, or products or services offered, on these sites, or the organizations sponsoring the sites.

This Guide was printed by the Massachusetts Elder Identity Theft Coalition under award #2016-XV-GX-K004, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this Guide are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

TABLE OF CONTENTS

Introduction	1
What is Financial Exploitation?	2
Telemarketing, Telephone Scams, & Robocalls.....	4
Unsolicited Mail & Unwanted Email.....	12
Online Tips	16
Door-to-Door	17
Charity Scams.....	19
Identity Theft	20
Resource Appendix	24
Attorney General’s Office Hotlines.....	32
Sources	34
Notes	35

INTRODUCTION

There has been an alarming increase of financial abuse against elders in the Commonwealth and throughout the United States. Financial exploitation of elders is all too common and unfortunately, it is only continuing to increase.

The fast-growing trend of elder fraud and the increasing number of financially victimized elders are of great concern to the Attorney General's Office (AGO). While the AGO prosecutes many companies and individuals that are committing these crimes, seniors and their families and friends are often in the best position to prevent fraud from occurring in the first place. This guide was created to help you protect yourself and your loved ones.

Included in this guide are some of the most common scams targeting elders that are reported to the AGO. Scams can materialize in many different ways and this guide provides warnings signs of scams, what to do should you become a victim, and useful resources throughout the state and country.

This guide covers scams that are usually perpetrated by individuals who are strangers to the elder. Unfortunately, it is all too common for elders to be abused by people who are close to them, including family members and caregivers. This guide does not address this kind of abuse, but if you are concerned that you or someone you know in this situation, please call the Elder Abuse hotline at the Executive Office of Elder Affairs: (800) 922-2275.

The AGO is pleased to present you with this guide and urge you to read it closely and refer to it whenever necessary.

WHAT IS FINANCIAL EXPLOITATION?

The financial exploitation of elders is the improper or illegal use of an elder's financial resources through, but not limited to, deceit, coercion, or undue influence of the elder. There are common scams that target elders, which are described in this guide, but exploitation can take on many different forms. Use this guide to learn how to spot financial exploitation, prevent it, and recover from it.

If you are a victim or suspect someone may be a victim of financial exploitation, or any type of abuse:

- Do not be critical of yourself or of someone who is a victim
- Seek assistance from
 - Someone you trust: children, relatives, or an attorney
 - Your local police department
- Contact the Elder Abuse Hotline: (800) 922-2275
- Contact the Executive Office of Elder Affairs
 - Phone: (800) AGE-INFO (800-243-4636)
 - TTY: (800) 872-0166
 - Online: www.mass.gov/elders
- Contact the Office of the Attorney General's Elder Hotline
 - Phone: (888) 243-5337
 - TTY: (617) 727-4765
 - Online: www.mass.gov/ago/elders

Tips to Prevent Elder Abuse

- Avoid isolation, stay active, and socialize with your family and friends.
- Monitor your financial transactions closely and confide in people you trust.
- Keep important legal and financial documents in a safe place.
- Do not engage with callers who try to pressure you into making an immediate decision.
- Be aware of current scams and identity theft methods.
- Safeguard your personal information and passwords.
- Be careful when responding to any solicitation – if it sounds too good to be

true, it most likely is.

- Screen your calls and only answer when you recognize the name/number.
- Never give out personal information over the phone, text, or email unless you initiated the conversation.
- Avoid getting on mailing lists and do not fill out contest entry forms.

Examples of financial exploitation

- Someone lies to you to convince you to give them money.
- Someone withdraws money from your checking account without permission or authorization;
- Someone forges your signature on a financial document;
- Someone misuses or steals your money or possessions;
- Someone that promises a large amount of money, but only if you send money immediately;
- Offers where the telemarketers want personal information before giving you more details on an offer;
- Coerced transfers of real estate; and
- Harassment by debt collectors.

Signs of financial exploitation

- Having difficulty buying groceries or paying household and utility bills.
- Accounts frequently being overdrawn or showing suspicious activity.
- Receiving a lot of mail about contests, sweepstakes, etc.
- Frequently getting calls from strangers offering great deals or asking for personal information.
- Receiving large numbers of magazines that you are not subscribed to
- Contact from debt collectors regarding unfamiliar debts.

TELEMARKETING, TELEPHONE SCAMS, & ROBOCALLS

Many elders find themselves constantly receiving unwanted telephone calls, some of which may be scams. While the unwanted calls can be difficult to stop completely, there are steps that you can take to lessen these annoying calls and protect yourself from these scams.

The “Grandparent Scam”

If you get a call from a young man or woman who says they are your grandchild, in trouble, and need money, try not to panic. It is likely a scam.

How It Usually Works:

- The con artist will start a conversation with something like this: “It’s me, grandma (or grandpa), your favorite grandson” and the unsuspecting victim may reply with the name of their grandson. The imposters will probably be crying and very upset. They will then tell you that they either lost a wallet, they’ve been arrested, they were in a car accident, or they are in the hospital, and they need money.
- Whatever the situation, they claim to be in crisis and invoke the love of a grandparent to give them money. They will very likely say they can only make one phone call and will probably beg you not to call their parents because they do not want them to find out and get upset.
- This scam is designed to prey on your emotions and create a sense of urgency. The scammer does not want you to take time to verify the facts.

What Should You Do?

- Remain calm, the scammer is hoping that you’ll act out of emotion.
- Hang up the phone. Call your grandchild and his or her parents and continue calling family members until you can confirm your grandchild’s whereabouts. Chances are you will discover that your real grandchild is safe and sound.
- Never wire funds, send cash, or purchase prepaid cards to send to the impersonator.
- Consider developing a code word with family members that can be utilized to verify an honest and true emergency.
- Make note of the caller’s phone number, the time of the call, and the date.
- Report scams to the Federal Trade Commission (FTC):
 - Phone: (877) FTC-HELP (877-382-4357)
 - Online: www.FTC.gov/complaint
- Call the Attorney General’s Office (AGO) Elder Hotline (888) 243-5337

Lottery & Sweepstakes Scam

Be wary about any calls you receive that claim you have won money or a prize. Have you entered any lotteries or sweepstakes lately? Does it sound too good to be true? Remember: if it sounds too good to be true, chances are it is probably a scam.

How It Usually Works:

- The scammer will call you and say something like: "Congratulations! You have won a lottery/sweepstakes/grand prize, but to claim your winnings, you must send a payment to pay the taxes and fees on the money you have won."
- They will try to convince you that there has been an administrative oversight of some kind and that you are in fact the winner of a large sum of money. Do not fall prey to their scams.

What Should You Do?

- If a telemarketer asks you to pay for a prize, hang up the phone immediately.
- Make note of the caller's phone number, the date, and time of the call.
- Do not send cash, checks, or wire money to pay taxes or fees to collect a prize or sweepstakes. You should never have to pay money to collect winnings.
- Ignore all calls, delete any voicemails, and throw away any mail that you receive that tells you you've won.
- Contact the FTC:
 - Phone: (877) FTC-HELP (877-382-4357)
 - Online: www.FTC.gov/complaint
- Call the AGO's Elder Hotline (888) 243-5337.

Tech Support Scam

You get a phone call or a pop-up ad on your computer that informs you a virus has been found on your computer. This person may tell you that they work with a well-known technology company and they need to access your computer to remove the virus.

How It Usually Works:

- The scammer will try to convince you the virus will cause your computer to shut down and to give them access to your computer.
- If you give them access, the scammer will search your computer for financial and personal information while they tell you they are removing the fake virus.
- After they have removed the fake virus, the scammer may demand payment.

What Should You Do?

- Never allow anyone who calls you unsolicited remote access to your computer.
- If you think there's a real issue with your computer, contact a professional yourself.
- If you have given someone access, you could become a victim of identity theft. See the identity theft portion of this guide for more information.
- Contact the Internet Crime Complaint Center (IC3) to file a report:
 - Online: www.IC3.gov
- Call the Attorney General's Elder Hotline at (888) 243-5337.

Government imposter scams

Be cautious about any calls you may receive from people claiming to be from Medicare, the Government, or the Internal Revenue Service (IRS). Many scammers will call elders pretending to be a representative of one of the listed organizations. Always remember, actual representatives from these organizations will never ask you for personal information or demand payment over the phone. It is a scam.

How It Usually Works:

- You will get a call from someone claiming to be calling from a government agency, like the IRS, Social Security, or Medicare.
- They may claim that you owe the government money and need to pay it by sending a wire transfer or purchasing pre-paid gift cards. Or, they may claim that there is a problem with your account and they need your social security or bank account number.

What Should You Do?

- The government will not request payments from you over the phone or in the form of a wire transfer or pre-paid card. Make note of the caller's phone number, the time of the call, and the date.
- Never give your personal information out over the phone unless you initiated the call.
- Report scams to the FTC:
 - Phone: (877) FTC-HELP (877-382-4357)
- Report IRS scams to the Treasury Inspector General for Tax Administration (TIGTA) at www.treasury.gov/tigta.
- Call the Attorney General's Elder Hotline: (888) 243-5337.

Fake Debt Collectors

Be on guard if you receive calls from people claiming that you owe a debt. These scammers will call elders and falsely claim to be a representative of a law office, a law enforcement agency, a debt collector, or creditor. Actual debt collectors are obligated under Federal and State laws to provide you with their business name, mailing address, and phone number. They cannot claim that they can have you arrested.

How It Usually Works:

- The fake debt collector will call you and claim that you or your spouse have a seriously delinquent debt and that you will be arrested if you do not pay it off immediately.
- Scam debt collectors may not tell you their office address, may threaten you with arrest or other penalty, and deny your request for debt verification in writing. Real debt collectors are required to provide this information.

What Should You Do?

- If you receive a call like the one described above, tell the caller that you dispute their claim and demand that they send you verification of the debt in writing. If they do not comply, it may be a scam.
- Never give your personal or financial information over the phone unless you initiated the call.
- Make note of the caller's phone number, the time of the call, and the date.
- File a complaint with:
 - The Attorney General's Elder Hotline: (888) 243-5337
 - The FTC: Phone: (877) 382-4357
Online: www.FTC.gov/complaint

Robocalls

Be wary about telephone calls and messages that are a recorded message or a robotic sounding voice. These are often scams and lead to even more unwanted phone calls.

How It Usually Works:

- You will receive a call or message from a robotic voice. It could be offering any number of services.
- Typically, there will be an option at the end of the call or message that prompts you to press '0' to either unsubscribe or to talk to an Operator to unsubscribe that way.

What Should You Do?

- If you receive one of these calls or messages, hang up or delete the message immediately.
- Do not press '0' or any other number. Pressing a number typically indicates to the scammers that your phone number is a valid working number. That usually means that they will continue to call and leave you these messages.

Please keep in mind that there are legal uses of automated calls, including:

- Calls and messages that are simply informational, i.e. message about doctor's appointments, flight delays, school closings, prescription refill reminders;
- Calls and messages from banks, telephone carriers, debt collectors, and charities; and
- Calls and messages from political candidates and organizations.

How to Prevent Unwanted Telephone Calls

- Contact the Federal Trade Commission and ask that your name be placed on the National Do Not Call Registry. All names that are added to the registry must stay there permanently unless they are requested to be removed. Joining the Do Not Call Registry is free and is available for both home and cell phone numbers.
 - To add your number to the National Do Not Call Registry:
 - Phone: (888) 382-1222
 - TTY: (866) 290-4236
 - Online: www.DoNotCall.gov (If you register online, you will receive a confirmation email from www.DoNotCall.gov. Click the link provided within 72 hours in order for your registration to be completed.)
 - Please Note: Putting your name on the National Do Not Call Registry does not take effect immediately. It usually takes about a month. Please be patient if you continue to receive calls in the following 31 days.
 - Please Note: The following calls are not screened by the Do Not Call Registry:
 - Calls from charities, political organizations, and people conducting surveys; and
 - Calls from companies that you've given permission to call you and with which you have an existing business relationship.
- Join the Massachusetts Do Not Call Registry. To add your number:
 - Phone: (866) 231-2255
 - Online: www.MADoNotCall.govconnect.com
- Never give out your personal information over the phone unless you initiated the phone call and know that you can trust the person or organization with whom you are speaking to. Legitimate companies or organizations will never ask for this information over the phone.
 - Do not provide the following information about yourself:
 - Social Security number
 - Credit card numbers
 - Bank account numbers
 - Simply tell the caller: "I do not give personal information out over the phone. I will be in touch with the company or organization directly and give them the needed information."

If You Continue to Receive Unwanted Telephone Calls

1. If you have joined the National Do Not Call Registry and you continue to receive unwanted calls after a month has passed, you can file a complaint with the Registry:
 - You must provide the date of the call and the name or phone number of the company that called you.
 - Phone: (888) 382-1222
 - TTY: (866) 290-4236
 - Online: www.DoNotCall.gov
2. File a complaint with the Elder Helpline through the Office of the Attorney General's Consumer Advocacy and Response Division:
 - In order to for our office to best help you, we ask that you provide the phone number of the telemarketer, the time of the call, and the date.
 - Phone: (888) 243-5337
 - Online: www.mass.gov/ago/complaint
3. Contact your local telephone service provider to inquire about blocking frequent unwanted numbers.

UNSOLICITED MAIL & UNWANTED EMAIL

Mail, Merchandise, & Email

Many elders find themselves frequently receiving unsolicited and unwanted mail, merchandise, and email. There are things you can do to reduce the amount of junk mail and email that you receive.

The U.S. Postal Inspection Service

If you believe you're a victim of fraud related to the U.S. Mail, including mailed sweepstakes, lotteries, on-line auctions, work-at-home scams, or chain letters, report your concern to the U.S. Postal Inspection Service as mail fraud.

U.S. Postal Inspectors investigate any crime in which the U.S. Mail is used to further a scheme—whether it originated in the mail, by telephone, or on the Internet. The use of the U.S. Mail is what makes it mail fraud.

- Phone: (877) 876-2455 then press '4'
- Online: <https://postalinspectors.uspis.gov/>

Unsolicited Mail

What Should You Do?

- Tell the companies with which you do business to remove your name from customer lists they sell to other businesses. To do this, look for information on how to opt out of marketing lists on sales materials, order forms, and businesses' websites.
- Utilize the services provided by the Direct Marketing Association to remove your name and address from most national telemarketing, mail, and e-mail lists. Contact the Direct Marketing Association ("DMA"):
 - Phone: (212) 768-7277
 - Online: <https://dmachoice.thedma.org/>
 - Mail: DMAchoice
Direct Marketing Association
P.O. Box 900
Cos Cob, CT 06087

Prescreened Credit & Insurance Offers

What Should You Do?

- In order to reduce the amount of preapproved credit card applications and insurance offers you receive, you can utilize www.OptOutPrescreen.com, the official Consumer Credit Reporting Industry website, to opt out either for five years or permanently:
 - To opt out for five years:
Phone: (888) 567-8688
Online: <https://www.optoutprescreen.com/>
 - To opt out permanently:
Visit www.OptOutPrescreen.com to begin the process
 - Please Note: When you call or go online, you will be asked to provide your name, telephone number, date of birth, and social security number. Your information is confidential and will only be used to process your request to opt out.
- If you do not have internet access, you can send a written request to each of the major credit reporting agencies. To opt out permanently, make sure your request includes your name, date of birth, home telephone number, and Social Security number.
 - **Experian**
Opt Out
P.O. Box 919
Allen, TX 75013
 - **Equifax, Inc.**
Options
P.O. Box 740123
Atlanta, GA 30374
 - **TransUnion**
Name Removal Option
P.O. Box 505
Woodlyn, PA 19094
 - **Innovis Consumer Assistance**
P.O. 495
Pittsburgh, PA 15230

Unordered Merchandise

What Should You Do?

- Occasionally, people will receive merchandise in the mail that they did not order. According to the FTC, you do not have to pay for any unordered merchandise that you may receive.
- If you receive unordered merchandise, there are a few things you can do:
 - You do not legally have to notify the seller, but it may be a good idea to contact them and let them know that you received something that you didn't order.
 - It's possible that you received the unordered merchandise as the result of a legitimate shipping error. In this case, contact the seller and offer to return the merchandise as long as the seller pays for shipping and handling costs.
 - Sometimes charitable organizations will send out items or samples that are noticeably marked free. You can keep these items as gifts.
- If you have further problems with receiving unordered merchandise first contact the company sending you the merchandise. If that doesn't work, contact:
 - The Elder Hotline at (888) 243-5337
 - U.S. Postal Inspection Service
 - Phone: (877) 275-2455 then press '4'
 - Online: <https://postalinspectors.uspis.gov/>

Unwanted Email

What Should You Do?

- Nearly everyone who uses e-mail has received unsolicited commercial messages, more commonly referred to as “spam.” To reduce the number of spam emails received:
 - Do not provide your email address on unknown websites, especially related to free trials or prizes.
 - Do not respond to emails where you cannot confirm or verify the sender of the email. “Phishers” send spam email claiming to be from a business or organization that you might deal with—for example, a bank, utility, online payment service, or even a government agency. By responding, you not only risk releasing your personal information, but also increase the chances of receiving additional emails.
 - Click ‘Unsubscribe’ at the bottom of the unwanted e-mail. Thanks to the CAN-SPAM Act of 2003, businesses that send commercial message are required to provide an unsubscribe option in all e-mails. Opt-out requests must be honored within 10 business days.
 - Opt out from most commercial “spam” emails by contacting the Direct Marketing Association (“DMA”):
 - Phone: (212) 768-7277
 - Online: www.DMAchoice.org
 - Mail: DMAchoice
Direct Marketing Association
P.O. Box 900
Cos Cob, CT 06087
 - File a complaint with the Internet Crime Complaint Center at ic3.gov
 - IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant.
 - Online: <https://complaint.ic3.gov/>

ONLINE TIPS

Tips to Keep You Safe Online

- Know who you are dealing with, especially when releasing personal information:
 - If you get an email or pop-up message asking for personal information, do not reply or click on the link in the message.
 - Avoid clicking on links or opening attachments from senders that you do not recognize, or that are in suspicious messages from people you do know, as they may have been a victim of a virus themselves.
 - The safest course of action is not to respond to requests for your personal or financial information. If you are releasing personal information with a merchant you are aware of, do not do so until you have checked for indicators that the site is secure, for example when you are online shopping. This includes an icon that looks like a lock on the browser's status bar or a website URL that begins "https:" (the "s" stands for "secure").
- Installing a firewall and antivirus software on your computer. It may protect your computer from viruses that can destroy or copy your data, slow down your computer's performance, cause a crash, or even allow spammers to send email through your own account. To be effective, make sure your anti-virus software is updated regularly.
- Back up your important files on a regular basis - just in case something happens to your computer, such as a virus, fire, theft, or damaging power surge.
- Be careful not to release too much information about yourself on the internet, especially on popular social networking sites like Facebook. Thieves may use such information to track your whereabouts, crack weak passwords, or take steps to commit identity theft.
- Create strong passwords, focusing on length and mix of characters. Try not to use any personal information in your password. Be careful about where you store your passwords and with whom you share them. Most importantly, make sure to change your passwords on a regular basis and do not use the same password on all sites.
- If you have a wireless network at home, be sure to protect it with a password to prevent unknown persons from trying to access your computer files. When dealing with public wireless, try to avoid transactions where you would release personal or financial information, such as online banking.
- If you are unfamiliar with how to do any of these tips, ask a trusted relative or friend for assistance.

DOOR-TO-DOOR

Many elders find themselves as the unsuspecting victims of Door-to-Door sales scams. It is important to know the signs so that you can easily avoid falling prey to these con artists.

Home Repair / Home Improvement Scams

Be on your guard if someone comes to your door offering any kind of home improvement or home repair services. They can be unlicensed and unregistered and may be trying to scam you out of your money.

How It Usually Works:

- Many scam artists will go door-to-door “selling” substandard work (driveway paving/repairs, chimney repairs, etc.) in exchange for your hard-earned money.
- They often approach seniors, claiming they have left-over materials from another job and offer services at a lower cost.
- This practice can leave you without the money you paid, with bad home repair work, and potentially costly repairs to fix what was supposedly fixed in the first place.
- These predators typically use high pressure tactics like “today only” deals or a claim that the need to repair is more urgent and serious than it really is. The purpose of the high pressure “sell” is to get you to agree to a verbal contract on the spot. The FTC “Cooling Off Rule” regulations require that someone selling door-to-door to inform you of your right to cancel the transaction, if you notify the seller in writing within three days of the sale.

What Should You Do?

- If someone comes to your door selling home repairs, first ask to see their license and permit to be soliciting in your town. If they cannot provide either, it may be a scam.
- You may also want to call your city or town hall and verify that they are licensed and permitted to be working in your town. Ask them to wait outside and do not let them in.
- Do not feel pressured to say yes or to make payment. Ask to see a sample contract and/or a list of their customer references. Tell them that you’ll consider their offer and get back to them if everything checks out.

- Your home is your most valuable asset; always err on the side of caution when hiring any potential contractors.
- The safest course of action is to not agree to any repair from someone who comes to your door and research any potential contractor before hiring them.

For more information about hiring a home improvement contractor, visit:
www.mass.gov/homeimprovement.

Competitive Electric Supply

A competitive electric supplier is a company licensed by the Department of Public Utilities to purchase electricity and sell it to retail customers. They are NOT your utility company. Your utility company automatically provides your supply of electricity when you sign up for their services. A competitive electric supplier may make it seem like they're a good deal for you, but the AGO has found that consumers who switched lost \$176.8 million dollars from 2015-2017, versus those who stayed with their utility company.

What Should You Know

- Your utility company is not allowed to make a profit on your supply of electricity. The price you pay (usually measured in kilowatt-hours) is the price they paid for it.
- Your utility company will not try to sell you on new supply options. If someone contacts you to change your electric supply and says they "work with" your utility company, they are likely a competitive electric supplier.
- You pay a fixed rate with your utility and the rate changes every six months. Sometimes the price from a competitive supplier may look like a better price, but it may be a variable rate that will go up later. Electricity price usually drop in the summer, so if you sign up with a competitive supplier in the winter, you may save money in the beginning but lose money over the course of the contract. There may be cancellation fees if you try to leave the contract early.
- Treat your utility account number like your social security or credit card numbers. An unscrupulous salesman could use your account number to sign you up for services without your authorization.

For more information on Competitive Electric Supply visit:
<https://www.mass.gov/competitive-electric-supply>.

CHARITY SCAMS

Many elders find themselves as the unsuspecting victims of Charity Scams. It is important to know the signs so that you can avoid falling prey to these con artists.

Charity Scams

Residents of Massachusetts are extremely generous when it comes to donating to charitable organizations, and elders are especially charitable. While most charities are honest, there are some organizations posing as charities that try to scam people out of their money.

How It Usually Works:

- You may receive a phone call, message, email, or piece of mail that encourages you to donate to some charity or another.
- These requests will often appeal to you emotionally, but not describe thoroughly where your money will go or how it will help those in need.
- They can often also be high-pressure demands for quick donations.
- Oftentimes, the name of the organization will sound very similar to a well-known and respected organization.

What Should You Do?

- If you receive something that is asking for donations, remember to do your homework. Research the organization as thoroughly as you can to make sure that they are legitimate. Feel free to contact them and ask for a background check on their charitable operations. Make sure the charity is registered by visiting the AG's Public Charities Annual Filings Website: www.mass.gov/ago/charities.
- Do not rush into giving away your hard-earned money because you are being pressured into donating. Find out exactly where your money will be going and whether most of it will actually go to help those in need or if it will go to administrative costs and advertising efforts.
- Do not give out your credit card number or bank account information over the phone. Do not give cash. Make sure to write the name of the actual charity on the check and get a receipt for your donation.
- For further information, visit the Office of the AG's Public Charities/Non-Profit Organization's resource page: www.mass.gov/ago/charities.

IDENTITY THEFT

Identity Theft & Medical Identity Theft

Identity theft is a form of theft in which someone assumes that person's identity for fraudulent purposes. Identity theft occurs when someone uses your personal information – such as your Social Security Number, credit cards, account numbers, or passwords, etc. – to defraud or commit crimes.

If you are a victim of identity theft, you may lose significant amounts of money and time. You may also find that your reputation and credit rating have been damaged, which affects your ability to obtain loans for education or housing, approval for rental agreements, and approval for credit cards or large purchases requiring credit.

How to Protect Yourself

- Credit Reports
 - Pay attention to the contents of your credit report to protect your financial status. You have the right to order a free annual credit report from Equifax, Experian, and TransUnion every twelve months to check the validity of your report's contents.
 - Phone: (877) 322-8228
 - Online: www.AnnualCreditReport.com
 - Because you are entitled to a free annual credit report from each company, it is recommended that you request a report every four months (alternating the credit reporting company) to monitor your credit activity.
- Don't become a victim
 - Carefully safeguard all personal information and be aware of potential scammers seeking to obtain and wrongfully use your personal information;
 - Keep your Social Security card in a safe place;
 - Refrain from giving out your personal information to anyone with whom you have never done business;
 - Watch your accounts for any unauthorized changes;
 - Check your credit report; and
 - Shred any documents that contain your personal information.

If you believe that you may be the victim of identity theft

Place an Initial Fraud Alert (good for one year) by contacting one credit reporting company. A fraud alert makes any potential creditor take additional steps to verify your identity before approving a new line of credit.

- Equifax:
 - (800) 525-6285
 - Online: Alerts.equifax.com
- Experian:
 - (888) 397-3742
 - Online: Experian.com/fraudalert
- TransUnion:
 - (800) 680-7289
 - Online: Transunion.com

You can also place a security freeze on your credit report. A security freeze stops any hard pull of your credit. A security freeze must be placed with each of the three credit reporting agencies individually. Keep in mind, a security freeze also stops you from opening a new line of credit. When you freeze your credit, you will get a pin number. Keep that safe and available, because you need it to unfreeze your credit if you want to use your credit.

Contacts for Security Freezes:

- TransUnion.com/freeze
 - 1-888-909-8872
- Experian.com/freeze
 - 1-888-397-3742
- Freeze.Equifax.com
 - 1-800-349-9960

Create an Identity Theft Report with the Federal Trade Commission

- Full Instructions can be found here: www.consumer.ftc.gov/articles/0277-create-identity-theft-report
- Monitor Your Progress
 - Resolving identity theft takes phone calls and letters. Create a system to organize your papers and calls, and to track deadlines.

Medical Identity Theft

Medical identity theft occurs when someone uses your personal information, without your knowledge or consent, to obtain or receive payment for, medical treatment, services, or goods. Victims of medical identity theft may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits.

In addition to risks of financial harm common to all forms of identity theft, the thief's medical history may be added to the victim's medical records and can involve the creation of fictitious medical records in the victim's name.

Inaccurate information in the victim's records is difficult to correct and may affect future insurability or cause doctors relying on the misinformation to deliver inappropriate medical care.

Signs of Medical Identity Theft:

- A bill for services you didn't receive;
- A call from a debt collector about a debt you do not recognize;
- Medical collection notices on your credit report that are not yours; and
- A denial of insurance for a service you should receive.

What Should You Do?

- Closely monitor any "Explanation of Benefits" sent by public or private health insurers. If anything appears wrong, raise questions with the insurer or the provider. Do not assume that there are no problems simply because you may not owe any money.
- Request a listing of benefits paid in your name by any health insurers that might have made such payments on your behalf. Do this once a year (or more often, if you believe there is cause for concern).
- Monitor your credit reports with the nationwide credit reporting agencies listed above (Equifax, Experian, and TransUnion) to identify reports of medical debts.
- Request copies of your current medical records from each health care provider and review your records for inaccuracies. Note that you will likely have to complete a form and pay a fee for a copy of these records.

Other Keys to Protection

- Guard your insurance card numbers as carefully as social security numbers.
- Do not share medical or insurance information by phone or email unless you initiated the contact and know who you are dealing with.
- Request full copies of health care files from all your providers.
- Pro-actively request and review an annual listing of all benefits paid by insurers.
- Review your medical records and report any errors to your health care provider and health insurer.
- If you find something unusual, alert your medical provider, investigate and suggest to your medical provider to add a “red flag alert” in your health care record to alert providers and insurers of potential fraudulent activity.
- Keep all copies of your records in a safe place and shred outdated documents.
- Remove personal information from pill containers before disposing of them. Many hospitals also have ‘Take-Back Prescription Drug’ days where you can dispose of medication and containers safely and securely.

RESOURCE APPENDIX

Office of the Attorney General

Attorney General Maura Healey is the chief lawyer and law enforcement officer of the Commonwealth of Massachusetts. In addition, her office is an advocate and resource for the Commonwealth and its residents in many areas, including consumer protection, combating fraud and corruption, protecting civil rights, and promoting meaningful economic recovery.

The Office of the Attorney General (AGO) is organized into six Bureaus: Executive; Health Care and Fair Competition; Criminal; Government; Energy and Environment; and Public Protection and Advocacy. Each bureau is divided into divisions and teams. These Bureaus and Divisions have distinct missions but work closely together to ensure the Attorney General's Office provides the highest level of public protection.

Consumer Advocacy and Response Division (CARD)

The AGO has dedicated and trained professionals in the Consumer Advocacy and Response Division (CARD) who can assist consumers in resolving a complaint through consumer advocacy services. CARD offers referrals to appropriate AGO divisions, other government agencies or outside organizations for complaints it cannot handle.

- Phone: (617) 727-8400
- TTY: (617) 727-4765
- Online: www.mass.gov/ago/complaint

Elder Hotline

The Elder Hotline provides a central place where senior citizens and their families receive information, referral, and mediation services.

- Phone: (888) AG-ELDER (888-243-5337)
- TTY: (617) 727-4765
- Online: www.mass.gov/ago/elders

Health Care Division

The Health Care Division works to promote public health and to improve the efficiency and effectiveness of the health care system. The Division has conducted groundbreaking examinations of health care cost trends and cost drivers that have directly led to new laws that have increased the transparency of the health care market and encouraged more efficient health care purchasing. The Division also provides guidance and public reporting on the community benefits offered by nonprofit hospitals and health plans through the innovative Community Benefits Program.

The Health Care Division also operates a health care helpline to help consumers understand their health care rights and to mediate consumer disputes with health care payers and providers. The Division receives and responds to thousands of helpline calls and written complaints each year.

- Phone: (888) 830-6277
- Online: www.mass.gov/ago/complaint

Executive Office of Elder Affairs

The Executive Office of Elder Affairs is the main resource for elders in the Commonwealth. Within it are programs designed to help elders in just about every aspect of their everyday lives.

- Phone: (800) AGE-INFO (800-243-4636)
- TTY: (800) 872-0166
- Online: www.mass.gov/elders ; www.800AgeInfo.com
- Elder Abuse Hotline: (800) 922-2275

Housing – www.mass.gov/elders/housing

- Assisted Living
- Congregate Housing
- Continuing Care Retirement Communities (CCRC)
- Reverse Mortgage Counselors
- Supportive Housing

Home Care – www.mass.gov/elders/homecare

- Aging Service Access Points (ASAPs)

Meals & Nutrition – www.mass.gov/elders/meals-nutrition

- Elderly Nutrition Program
- SNAP for Seniors
 - Phone: (866) 950-FOOD (866-950-3663)

Service Organization & Advocates – <https://www.mass.gov/advocacy-services>

- Aging Service Access Points (ASAPs)
- Area Agency on Aging
- Assisted Living Ombudsman
- Community Care Ombudsman
- Councils on Aging
- Long Term Care Ombudsman
- Protective Services
 - Elder Abuse Hotline: (800) 922-2275

Caregiver Support – www.mass.gov/elders/caregiver-support

- Massachusetts Family Caregiver Support Program

Elder Abuse & Protective Services Program

Elder Affairs has established 22 designated Protective Services (PS) agencies throughout the Commonwealth to respond to reports of elder abuse.

- Elder Abuse Hotline: (800) 922-2275
- Online: <https://www.mass.gov/reporting-elder-abuse-neglect>

Elder abuse includes physical, emotional and sexual abuse, neglect by a caregiver, self-neglect and financial exploitation. The goal of protective services is to remedy or alleviate the abusive situation and to prevent the reoccurrence of abuse.

Health Care

Other Health Care Resources include:

- Medicare Advocacy Project
 - Phone: (800) 323-3205
 - Online: <https://mlac.org/funding/appropriated-projects/>
- MassHealth
 - Phone: (800) 841-2900
 - TTY: (800) 497-4648
 - Online: www.mass.gov/masshealth
- Prescription Advantage
 - Phone: (800) 243-4636
 - TTY: (877) 610-0241
- Serving the Health Information Needs of Elders (SHINE)
 - Phone: (800) AGE-INFO (800-243-4636) and then press '3'
 - TTY: (800) 872-0166

Massachusetts Senior Legal Helpline

The Massachusetts Senior Legal Helpline is a project made in collaboration with the Massachusetts Office of Elders Affairs and Volunteer Lawyers Project of the Boston Bar Association.

- Phone: (866) 778-0939
- Online: www.mass.gov/elders/senior-legal-helpline

The Helpline provides FREE legal information, advice, and referral services for Massachusetts senior citizens (60 years or older) in most areas of civil law, including:

- Social Security / SSI
- Veterans Benefits
- Mass Health
- Medicare
- Consumer issues
- Public Benefits
- Unemployment
- Foreclosures
- Guardianship
- Powers of Attorney
- Bankruptcy
- Evictions
- Landlord/Tenant
- Utilities
- Family law
- Nursing Home

The Helpline also provides interpretation services in many languages.

H.O.M.E. – Homeowner Options for Massachusetts Elders

A charitable nonprofit agency, H.O.M.E. is dedicated to protecting the equity of low and moderate income elder homeowners. As an independent third party, H.O.M.E. does not charge fees to its clients nor receive considerations for any possible financial transactions. This allows H.O.M.E. counselors to focus solely on H.O.M.E.'s mission:

To assist low- and moderate-income elder homeowners successfully age-in-place.

Recognized as a national leader in senior foreclosure prevention, H.O.M.E. provides the only statewide in-home counseling service of its kind.

- Phone: (800) 583-5337
- Online: www.ElderHomeowners.org

Federal Government Resources

Medicare

- Phone: (800) 633-4227
- Online: www.medicare.gov

Social Security

- Phone: (800) 722-1213
- Online: www.SocialSecurity.gov

LifeCare Advocates

Founded in 1993 by Emily B. Saltz, LICSW, LifeCare Advocates is recognized on a local and national level as a leader in elder care. If you are a family member who is coping with the stresses of caring for an elder relative, Elder Resources can help.

- Phone: (617) 928-0200
- Online: www.EldersMA.com

An experienced staff of Geriatric Care Managers offers highly personalized services, acting as an essential link between our clients and the services they need. Whether you are a family member caring for an elder relative, or a professional considering the appropriate resources for your clients, LifeCare Advocates offers guidance you can count on.

Senior Resource Center, Inc.

Senior Resource Center, Inc. (SRC) provides an all-inclusive approach to protecting not only a family's financial resources but also the invaluable assets of dignity and quality of life.

- Phone: (617) 472-6600 ; (888) 869-6295 (toll-free)
- Online: www.HelpingElders.com

ElderCare Resource Services

ElderCare Resource Services is a Geriatric Nurse/Social Worker partnership that assists families in investigating, assessing, and recommending the medical and non-medical resources required for the care of Seniors. We are strong advocates for our clients, delivering the information and resources necessary to make them the best consumers and ensuring their relative the best possible care.

- Phone: (508) 879-7008 ; (866) 280-2308 (toll free)
- Online: www.ElderCareResourceServices.com

Mass Home Care

Mass Home Care wants to help you and your family age well. Instead of spending hours searching for the right service, let them put the pieces together for you. They are a network of 30 non-profit "Age Info Centers." They cover every city and town in Massachusetts, and advocate for community care. We make a confusing system easy to use.

- Phone: (978) 502-3794 ; (800) AGE-INFO (800-243-4636)
- Online: www.MassHomeCare.org ; www.800AgeInfo.com

Boston Elder Info

Boston ElderINFO assists elders, disabled individuals and their families in accessing a comprehensive range of services that address health care needs.

- Phone: (617) 292-6211
- TTY: (617) 451-6404
- Online: www.ElderInfo.org

The LGBT Aging Project

A non-profit organization dedicated to ensuring that lesbian, gay, bisexual and transgender older adults have equal access to the life-prolonging benefits, protections, services and institutions that their heterosexual neighbors take for granted.

- Phone: (617) 522-1292
- Online: www.LGBTAgeingProject.org

Aging Organizations and General Interest

- AARP www.aarp.org
- Administration on Aging www.aoa.gov
- AGS Foundation for Health in Aging www.healthinaging.org
- American Geriatrics Society www.americangeriatrics.org
- American Society on Aging www.asaging.org
- Benefits Check Up www.benefitscheckup.org
- Boomerater www.boomerater.com
- Eldercare Locator www.eldercare.gov
- Federal Consumer Information Center www.pueblo.gsa.gov
- Gerontological Society of America www.geron.org
- Global Action on Aging <http://globalag.igc.org>
- National Association of Area Agencies on Aging www.n4a.org
- National Council on the Aging www.ncoa.org
- National Hispanic Council on Aging www.nhcoa.org
- National Institute on Aging www.nia.nih.gov
- SeniorDiscounts.com www.seniordiscounts.com
- SeniorJournal.com www.seniorjournal.com
- The Seniors Coalition www.senior.org
- Suddenly Senior www.suddenlysenior.com
- ThirdAge www.thirdage.com
- WiredSeniors wired-seniors.com

ATTORNEY GENERAL'S OFFICE HOTLINES

Elder Hotline: (888) 243-5337

The Elder Hotline offers both hotline and advocacy services to Massachusetts' senior citizens, their families, and related caregivers seeking assistance with consumer-related issues. The hotline is staffed by interns and volunteers providing dispute resolution services and is a comprehensive resource for information and referrals.

Monday through Friday 9am to 5pm.

Civil Rights Division: (617) 963-2917

The Civil Rights Division (CRD) enforces state and federal laws that protect residents of and visitors to the Commonwealth from discrimination on the basis of race, national origin, gender, sexual orientation, veteran status, disability, or any other protected status. Anyone who believes that they are a victim of discrimination (in such areas as housing, employment, and public accommodation, for example), can file a complaint with the CRD.

Monday through Friday 9am to 5pm.

Consumer Hotline: (617) 727-8400

The Consumer Advocacy and Response Division (CARD) handles questions and concerns in the area of consumer protection. Consumer Specialists on the hotline will answer consumer related questions, offer referrals to the appropriate AGO divisions, other government agencies, local consumer programs, face to face mediation programs or other organizations. CARD provides a free, consumer advocacy service that tries to help resolve matters between consumers and merchants outside of court.

Monday through Friday 10am to 4pm.

Fair Labor Hotline: (617) 727-3465

The Fair Labor Division protects employees from exploitation by employers. Through prosecutions, civil suits and administrative proceedings, the division enforces the Commonwealth's wage and hour laws, including the prevailing wage, minimum wage, payment of wages, overtime, retaliation, tip pooling, child labor, and Sunday and holiday premium pay laws. The Fair Labor Hotline is available to help workers file wage complaints.

Monday through Friday 10am to 4pm.

Insurance Fraud Tipline: (617) 573-5330

This tipline is available 24 hours a day and takes calls pertaining to reports of fraud in any of the following areas: workers' compensation, motor vehicle insurance, disability, health care billing and unemployment insurance.

24 hour voice messaging system.

Insurance & Health Care Consumer Helpline: (888) 830-6277, ext. 3

This helpline is available to assist consumers who have questions or are seeking assistance with issues related to health care, health insurance and/or automobile and motorcycle insurance. The Insurance and Financial Services Division also houses the AGO's Student Loan Assistance Unit.

Monday through Friday 9am to 5pm.

Medicaid Fraud Tipline: (617) 963-2360

This tipline is available 24 hours and is intended for calls pertaining to abuse or neglect of a Long-Term Care Facility resident or fraud committed by a Medicaid provider.

24 hour voice messaging system.

Victim Compensation Hotline: (617) 727-2200 ext. 2160

If you are a victim of violent crime, you have certain rights under Massachusetts Law, and you are eligible for certain services. The AGO is committed to empowering crime victims and providing them with the tools and support they need to begin the healing process.

Monday through Friday 9am to 5pm; and 24-hour voice messaging system (staff member will return calls during business hours)

Victim Witness and Assistance Division: (617) 727-2200

Provides crisis assessment and intervention to victims and witnesses to facilitate their emotional, psychological, physical and financial recovery from victimization; aims to reduce the level of secondary victimization associated with victims' and witnesses' involvement in the justice system and other collateral systems; and ensures that victims and witnesses are provided with the rights and services mandated by the Victim Rights Law.

Monday through Friday 9am to 5pm. Please call number listed above, press zero for the operator, ask for the Victim Witness and Assistance Division.

SOURCES

Information for this Guide was provided by the following Agencies and Organizations:

- Better Business Bureau
- Boston Elder Info
- ElderCare Resource Services
- Executive Office of Elder Affairs of Massachusetts
- Federal Bureau of Investigation
- Federal Trade Commission
- Fraud.org
- H.O.M.E. – Homeowner Options for Massachusetts Elders
- LGBT Aging Project
- Mass Home Care
- Massachusetts Elder Resources
- Massachusetts Office of Attorney General
- Massachusetts Senior Legal Helpline
- Senior Resource Center
- United States Government
- United States Postal Inspection Service
- United States Postal Service

NOTES



MASSACHUSETTS OFFICE OF ATTORNEY GENERAL

One Ashburton Place

Boston, MA 02108

(888) 243-5337

www.mass.gov/ago/