New York State Office of the Attorney General

Smart Seniors

Letitia James
Attorney General

Letitia James
New York State Attorney General

Dear New Yorkers,

Stay Safe. Take Control. Fight Back.

Being a smart consumer requires having the tools to protect yourself from fraud and abuse. Unfortunately, there are many ways for con artists and other criminals to gain entry into our lives: over the phone, through the internet, sometimes in our own homes. And too many of them make it a practice to target elderly New Yorkers.

This booklet is aimed at helping you stop scam artists and abusers before they strike by informing you of your rights and laying out the steps you can take to protect your assets and your health. From making smart purchasing decisions to planning your health care, from recognizing crimes to knowing how to fight them, it's important that you know the best ways to protect yourself.

One of our office's most important functions is protecting New Yorkers from fraud and abuse. If you believe that you or someone you know have been victimized, call us. We have investigators and prosecutors who specialize in fighting consumer fraud, neglect and abuse, and problems in the health care system. We will try to answer your questions and provide the help you need.

Sincerely,

Letitia James

Letitia James

Table of Contents

		Page
I.	Anatomy of a Scam	1
II.	Common Scams	2
III.	Internet Safety	6
IV.	Identity Theft	8
V.	Charities	11
VI.	Elder Abuse and Neglect	12
VII.	Medicaid Fraud Control Unit	14
VIII.	Take Control of Your Finances; Your Health	15
	Resources	18

Stay Safe • Take Control • Fight Back

Fraud and abuse against the elderly takes on many shapes and forms. It ranges from home improvement scams to medicaid fraud to physical abuse. It costs its victims nearly $3 billion each year.

That's why it's important that people are armed with the information they need to stay safe, that they have the tools to take control of planning for their financial and physical well-being and that they know where to go for help or to report a crime.

I. Anatomy of a Scam

It can be fraud, physical abuse or financial embezzling, most crimes that take advantage of a person's trust have the same components and most have roots in the basic scam or con.

Technology may advance, the appeals may become global, but the structure of a scam is unchanging. Whether it is someone trying to sell you a new roof or an email claiming you won a lottery you don't remember entering, there will be common elements to a scammer's pitch.

The first step is to know what a scam looks like. Watch out for these when someone is offering you a deal or making a request:

1. **The Distracting "Hook":** At the center of a scam there's always something to get your attention, to appeal to you in a way that causes you to pay less attention to the details, or to let your guard down.

2. **A Con Artist Who Seems Trustworthy**: Most people trust unless they've been given reason not to. Scammers are very good at manipulating people into trusting them.

3. **A Deadline:** This might be a dead giveaway that you are looking at a scam. Most legitimate marketing campaigns have a hook, something to entice a buyer. Most advertising campaigns count on you trusting their facts. If something is not going to be around tomorrow, it is likely not legitimate.

Scam artists use a "hook." Chances are good it will be one of these:

- **Money or Greed** Most of us look for a good deal or dream of sudden riches.
- **Love or Good Will** Good people want to help those they care about.
- **Fear and Desperation** Ironically, being afraid can make us less cautious, more open to the promise of a quick fix or unexpected cure.

II. Common Scams

It is illegal for any sweepstakes or lottery to:

- Claim that you are a winner unless you have actually won a prize;
- Require that you buy something to enter the contest or to receive future sweepstakes mailings, or imply that your chances of winning are better if you make a purchase;
- Mail fake checks that do not clearly state that they are non-negotiable and have no cash value;
- Use seals, names or terms that imply government affiliation or endorsement;
- Conduct a lottery over the phone or through the mail.

Sweepstakes or Contests

Sometimes it's a "Foreign Lottery" or a "Random Drawing" or "Millionth Customer" that entitles you to a cruise, money or new computer. The news might come over the phone, through the mail, or over the internet.

Common Components of the Sweepstakes Scam:

- A request for the "winner" to send a check or to wire money to cover taxes and fees. Sometimes the contest notification includes a check that the winner is to deposit; the winner is directed to send back a percentage of the money. Legitimate contests never ask for money upfront.
- A request for your banking information in order direct deposit your winnings. This is an attempt to steal your identity. They will wipe out your bank account.
- Using a name which sounds like a government agency or official-sounding authority. The name can be invented: like the "National Sweepstakes Bureau," or "The National Consumer Protection Agency." Neither of these exists. Sometimes they will use an actual name like the Federal Trade Commission. The scammers claim that the government "oversees" the integrity of foreign lotteries. They do not. This is a scam.

Stay Safe, Take Control:

- Never wire money to someone you don't know who contacts you; it's the same as handing over cash.
- Never pay to collect prize money, whether they ask you to wire money, or send a check to "cover" the taxes or another form of payment. Legitimate lotteries and sweepstakes deduct the amount you owe the IRS from the winnings, and you will fill out multiple forms directly with the IRS.
- Don't rely on Caller ID. Scammers use technology to make you believe a call is coming from your area or from Washington, DC.
- Be a friend. If you suspect a friend or family member is being scammed, try to talk to them about it. Some signs are

THIS DOCUMENT HAS AN OFFICIAL WATERMARK PRINTED ON THE BACK. THE FRONT OF THE DOCUMENT HAS A MICRO PRINT ABSENCE OF THESE FEATURES WILL INDICATE A COPY.

usbank
Five Star Service Guaranteed

FAKE!!!!! CHECK

No. 52239085

935-41
920

DATE:
3/21/08

PAY Eleven Thousand Five Hundred Dollars

$ 11,500.00

TO THE ORDER OF: Lynn Stewart

PURPOSE/REMITTER: [redacted]

Location: 4937

Issued By: MoneyGram Payment Systems, Inc. P.O. Box 9476, Minneapolis, MN 55480

AUTHORIZED SIGNATURE

stacks of "guaranteed winner" mail, packages containing jewelry, wristwatches or so-called "collectibles. "

Grandparent Scam

"Grandma, it's me...please don't tell Mom..."

Typically, this scam comes in the form of an urgent phone call. The caller claims to be "your favorite grandson" or just says "it's me"... prompting the grandparent to supply the needed name. While the emergencies vary, the scenario is usually this: the "grandson" is out of town and needs money fast -- to make bail, or to pay for automobile repairs or medical expenses. The caller begs the grandparent not to tell his parents. Just wire the needed money immediately.

Scammers know that parents and grandparents fear a call that tells them their loved one is in trouble. Each year, thousands of Americans get caught in the Grandparent Scam. Increasingly, scammers use actual relatives' names and information gleaned from social media and other internet sites. Don't fall for it.

Stay Safe, Take Control

- Never wire money to anyone without verifying their identity.
- Don't rely on recognizing a caller's voice; verify that you know the person on the other end.
- Tell the caller to give you the name and contact information of the law enforcement agency, hospital or car repair shop they are dealing with, and verify that the story the caller told you is accurate.
- Before sending money, speak to your family to find out if someone is actually out of town and in need of assistance.

The Fake Check

The fake check isn't limited to sweepstakes; you'll find it in "secret shopper" come-ons; sales or auctions; and work at home opportunities to name a few.

The mark is asked to deposit a check, and then wire part of the money back. Usually these checks look very real; in fact sometimes they are real checks.

The problem is that there is no money behind them. The check is deposited, and at least part of the money wired back to the scam artist. When the check bounces, the money wired is lost.

This scam works because you have to wire the money BEFORE the check clears.

Home Improvement Scams

Home contracting schemes are frequently aimed at senior citizens, perhaps because they are home more often, are likely to own their own homes, and own homes that may need repair. Some common approaches are:

"I'm doing work around the corner and have material left over. I can do yours for next to nothing."

The Drive-Bys

The contractor "just passing by" is one of the most common scams. Sometimes they claim to have done work a couple blocks away and have leftover material. Other times they notice something wrong: a tree branch down or some siding loose. In some cases, they actually cause the damage before offering to do the repairs.

These offers for quick, cheap repair usually result in low quality work such as watered down stain instead of paint, inferior shingles on only half the roof, or a thin smear of blacktop on the driveway. These scammers typically demand a payment upfront and, if they actually finish the job, it probably won't last.

Free Inspection Scams

Weather proofing, new windows, chimneys: since keeping our homes weather tight is a high priority, scammers will often offer "free inspections." They will almost always find a problem that needs an expensive solution: an expensive pump that needs to be installed; excavation work on the foundation to waterproof when cleaning the gutters would work; a new chimney; or new windows when some weather stripping would do the trick.

Stay Safe, Take Control

- Be suspicious about any unsolicited offer to work on your home. Remember, there is no problem so serious it can't wait a day or two for you to do some research.
- Ask your friends and neighbors about who they would recommend. Remember, the best contractors are found by word of mouth.
- Check out the contractor with the local Better Business Bureau.
- Get references.
- Use local companies whose address you can verify.
- Avoid unlicensed contractors. Some counties and

After The Storm

Be especially alert following major weather events, like blizzards or floods. Scammers will take advantage of the number of people who need repairs.

municipalities require contractors to be licensed.

- Get more than one written estimate, and make sure the estimates include details about the work and materials.
- Don't let a contractor work without the necessary permits and insurance.
- Don't assume the lowest estimate is the best deal. Check the quality of the materials.
- Get it in writing: a written contract is required by law for work costing more than $500.
- You have the right to cancel the contract until midnight of the third business day after the contract was signed. Cancellation must be in writing.
- Be clear that you won't pay for any work or changes in the contract unless it's agreed upon in writing.
- Never pay the full amount up front. Negotiate a payment schedule tied to progress on the job. Make sure the work is done according to the contract before you make the final payment.
- If possible, pay by credit card. Otherwise, pay by check. Never pay cash.

Dealing with Telemarketers

There are legitimate telemarketers and there are scammers, and there are some who fall in-between. The problem is that they all target people who are at home during the day and in the habit of answering their phones. It's important to keep your guard up when answering the phone. Here are some things to remember:

- **Don't rely on caller ID to let you know who the call is coming from**. Scammers often manipulate the caller ID to give you the impression that it is a local call, or from an "official" location, like Washington DC. Make sure you are familiar with the company or charity the caller is working for. If not, give yourself time to check it out before committing to a purchase or contribution.
- **Never give out personal information to an unsolicited caller,** that is, someone who initiates the contact with you. The information you should withhold includes your

Telemarketers are regulated:

- Calling hours are limited to 8am - 9pm.
- Telemarketers must tell consumers that they are trying to sell something and identify the actual seller.
- Before asking for money, they must disclose the nature of the products or services for sale, the costs, and any delivery restrictions.

birthdate, social security number (even the last four digits), your mother's maiden name, your first pet's name or anything that might be used as a password or other identifier. You can never be sure if the caller really is who they say they are.

- **You don't have to commit to anything on the phone**. Ask to see a proposal in writing, give yourself time to research or think about it. Go back to that anatomy of a scam: legitimate sales people will give you time to make a good decision.

III. Internet Safety

Social Networking

Sites like Facebook and Skype can be great ways to keep in touch with far flung family and friends. Unfortunately, scam artists also surf these sites looking for information.

- Use privacy settings and passwords.
- Make your photos and information available only to those you've "friended."
- Don't friend people you don't know.
- Don't post personal identifying information such as your birthdate, home address or phone number.

Online scams and identity theft are increasing problems as the internet becomes a larger part of everyone's lives. But there are a number of ways to stay safe and take control.

Create Strong Passwords

Make them easy for you to remember, but hard for others to guess. Don't use personal information like your birthdate, your Social Security number or your mother's maiden name. Also avoid obvious choices like the names of your children or pets. Include symbols and numbers, and use upper and lower cases.

Use different passwords for different scenarios. If someone breaks the code for your email, and it's the same for your banking information, you are at risk for losing a lot. Keep your passwords in a secure place. Passwords are important for:

- Wireless Internet Networks. If you have a wireless internet network set up in your home, secure it. Hackers roam communities looking for unprotected networks. If they log onto yours, they can easily break into the information on your computers. They can also use your internet network to conduct illegal business or download pornography and other material you don't want associated with your account.
- Each individual computer and each account on the computer should be password protected.
- Email. If you use your email for shopping, paying bills or banking, there is a lot of personal information that can be accessed with the click of button. If you have a smartphone, password protect that too.
- Other accounts. If you bank or shop online, you will be asked to register a username and password.

Use Secure Sites

Make sure that the sites you use for shopping and banking are secure. Here is how to tell:

Look at the name of the website as it appears in the browser bar. Make sure there is an "S" in the protocol at the beginning of the site's name. A secured site will start with https://.

Look for the security certificate on the browsers' window. That's where you type the name of the site you want to go to. Most browsers use a padlock icon like the one above. When you click on this, it will tell you the name of the owner of the certificate, which should be the same as that of the site you are on. Some browsers don't use the padlock icon; instead the name of the site will be highlighted in color before the https://. Click on the name to be sure it matches.

Don't use a debit or check card online, only credit cards. Debit cards, even those with a credit card name and logo, do not carry the same protections. If your credit card information is stolen, you are only liable for $50 in fraudulent charges. If your debit card information is stolen and the thief wipes out your bank account, the money is gone.

Don't be "Phished"

Phishing is an attempt to get a victim to provide personal information such as their username, password, or credit card number. The scammers typically masquerade as a familiar and trustworthy company, such as your bank, an online store where you have shopped previously, or your credit card company. Sometimes they pretend to be a government agency. They will send you an email claiming that there's a problem with your account and they want to help. Sometimes they will call you on the phone or send you a text. The key to the phishing scam is that they ask you to provide personal information, such as your social security number or password, so they can "confirm your identity" and then "straighten out your account."

- Don't ever give your personal information or passwords to someone who contacts you unsolicited.
- Do not click on a link in an email from someone you don't

know, no matter who they claim to be. You may be directed to a bogus, "look-alike" website that spoofs the website of the real company. Instead of clicking on the link, go to the browser bar and type in the web address of the company you are trying to reach. Then you can be sure that you're on the "real" website, not a bogus one.

- Avoid opening emails that appear to be spam. It's just better not to pursue it.
- If you get a call, text or email from a company claiming that there's a problem with your account, do not respond. Instead, hang up the phone, delete the text or email, and then contact the company yourself. Now you can be sure you're talking with the real company, not a scammer who's trying to "phish" you.

IV. Identity Theft

Free credit report

www.

annualcreditreport.com

or

1-877-322-8228.

Everyone is entitled to a free copy of their credit report each year. You can get yours by registering at this website or calling this toll free number.

If you see accounts or inquiries that you did not initiate or you don't recognize, it may indicate that someone else is using your identity.

Phone call solicitations; phishing; fake checks: many of these scams are after more than quick cash. They want to steal your identity.

Identity theft — stealing personal information to gain access to credit, bank accounts, even medical care — affects millions of people each year and costs billions of dollars. Its victims are from every neighborhood and from every income level and age group. And it can happen anywhere: thieves get hold of your personal information in the trash, at a store or restaurant where you've used a credit or debit card, at the doctor's office or over the internet.

Here are some ways to stay safe and protect your identity:

- Shred all papers containing personal information before you throw them away.
- Safeguard: Keep your information protected and private. When paying your bills, don't place the envelopes in an unlocked mailbox such as the one at the end of your driveway. Have checks direct deposited. Don't carry your Social Security card or too many credit cards. Use passwords on your accounts. Don't use public computers, like those at cafes or libraries, for financial

transactions. At home, keep your personal information in a secure place.

- Review your bank and credit card statements carefully each month to make sure there are no unauthorized charges or indications of fraudulent use. If you bank online, check your account even more regularly. The sooner you catch the problem, the better off you are.
- Destroy financial information that is expired or no longer needed before you throw it away. Shred paper work, cut up plastic.
- **Most important: Don't give out your personal information to someone you don't know.**

Telemarketing, Internet, Direct Mail:

Opt out of the Come-ons

There are ways to greatly reduce the number of unsolicited phone calls, mailings and internet offers you receive. Taking these steps can stop annoying intrusions into your life and limit your risk of identity theft.

NATIONAL
DO NOT CALL
REGISTRY

Do Not Call Registry:

1-800-382-1222

www.donotcall.gov

You can place your telephone number (both landline and cell phone numbers can both be registered) on the Do Not Call Registry. Within 31 days of when you register your number, telemarketers — with certain exceptions — must remove you from their call lists.

Registration does not expire. Your telephone number will remain on the Do Not Call registry until the number is disconnected and reassigned, or you choose to remove the number from the registry.

Exceptions: Even if you register your number with the Do Not Call Registry, calls from or on behalf of political organizations, charities, and telephone surveyors would still be permitted, as would calls from companies with whom you have done business, or those to whom you've provided express agreement in writing

Credit Bureaus or *Consumer Reporting Agencies*

These companies provide credit information about individual consumers. If you open a charge account, apply for a loan, or rent an apartment, chances are your credit record will be checked. In the United States, the four national bureaus are:

Experian
TransUnion
Equifax
Innovis.

You can find contact information for each of them in the Resources section on page 19.

Shred, Shred, Shred

One of the most important steps you can take to protect your financial identity is to make shredding a habit. You can purchase a low cost shredder about the size of a small trash can. Some banks and municipalities also offer either shred bins or "shred days".

Shred items containing this information:

- Social Security numbers
- Account numbers
- Financial information
- Passwords
- Credit Card information
- Your signature
- Medical records
- Legal records

to receive their calls. However, if you ask such a company to place your number on its own do-not-call list, it must honor your request. You should keep a record of the date you make the request.

Unsolicited credit and insurance offers:

1-888-5-OPT-OUT (1-888-567-8688)

www.optoutprescreen.com

This service is run by the four major consumer credit reporting companies. When registering you will be asked to provide your home phone number, name, date of birth and Social Security number. This information will be kept confidential.

Mail and Email

www.dmachoice.org

The Direct Marketing Association (DMA), a trade organization for businesses that use direct mail, provides a service in which consumers can opt out of receiving unsolicited commercial mail from many national companies for five years and emails for six years. After registering with the Mail Preference Service (MPS) or Email Preference Service (EMPS), your name will be put on a "delete" file and made available to member businesses, reducing much of your unsolicited mail and email. (It will not affect mail from organizations that are not members of DMA.) To register, go to the website (www.dmachoice.org) or mail your request with a $1 processing fee to:

DMAchoice
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512

V. Charities

Mix Generosity with Caution

New Yorkers donate over $10 billion to charitable organizations each year, with older New Yorkers being especially generous.

Most charities are honest in their methods of soliciting contributions. However, there are organizations that misuse fundraising methods, with the lion's share of donations going to the fundraiser rather than the programs. Other so-called charities are outright scams that play on the sympathies of well-meaning people who only want to help a good cause.

Here are some ways to make sure your charitable donations are going where you intend them to.

- Make sure you know the charity and understand its aims and programs. Scammers will frequently capitalize on the reputation of a well-known charity by changing the name slightly.
- Confirm that the charity is registered with the Attorney General's Office, as required by law.
- Find out what the charity will do with your money: how much of each donation supports programs, administrative costs and fundraising.
- Avoid charities that will not answer your questions or provide written information about its programs and finances.

36.9 ¢ of Each Dollar

That's the average amount that actually goes to the charity when it raises funds through telemarketing campaigns. Many charities across the state receive even less – and sometimes the charities actually lose money. The Attorney General's Charities website **www.charitiesnys.com** provides information about the fundraising firms that charities use, and how much of themoney raised actually goes to the charity.

Making the Donation

- Resist pressure to give on the spot. If you choose to listen to their appeal, ask how much of your donation will be used for charitable programs, and how much the telemarketer is being paid. Beware of claims that "all proceeds will go to charity."
- Avoid unsolicited emails. These are frequently scams and your response may make you vulnerable to identity theft and fraud.
- Use caution when donating via text and social media. Although legitimate charities are increasingly using social

Fundraising for Law Enforcement

Exercise caution before donating to a law enforcement organization through a telemarketer. Contact your local police or other agency to check on the identity of the group asking for your contribution. Report any solicitor who uses coercive or abusive tactics or who promises that your contribution will entitle you to better police protection.

media and texting for donations, you should always check to be sure that your contributions are going to established, reputable charities.

- Watch Out for Fake Invoices. Scammers often send out "overdue" statements. Confirm that you've actually made a pledge to the organization. This could be a scam.
- Never Give Cash. It's best to give your contribution by check made payable directly to the charity, or by credit card.
- **Most importantly! Never give your Social Security number or other personal information in response to a charitable solicitation.** Never give out credit card information over the phone to an organization you are not familiar with.

VI. Elder Abuse and Neglect.

It's a problem that cuts across race, religion, culture and income. It encompasses physical, emotional and sexual abuse, as well as neglect. No one wants to think they are vulnerable, but it's important to know the risks of becoming a victim.

Risk Factors for Victims:

- Illness, cognitive impairment or dementia
- Social isolation
- History of domestic violence (This is true whether the elderly person was a victim of violence or was an abusive parent or spouse.)
- Shared living arrangement
- Web of dependency

Look for the Signs: There are usually signs -- physical, social and financial--that things just are not right.

Physical signs can include:

- Unexplained injuries like bruises and welts, especially if they are on both sides of the body, as though someone has been roughly grabbed or restrained;
- Broken eyeglasses;
- Signs of over or under medication;
- Unusual weight loss;
- Dirty living environment;
- Poor personal hygiene.

Social changes to watch for:

- Otherwise outgoing person seems fearful and reluctant to engage with friends;
- Withdrawn effect;
- Self-destructive behavior;
- Emotional distress.

Financial Signals:

- Sudden changes in either the elder's or caregiver's financial condition;
- Items missing from the home;
- Unpaid bills which the senior should have the resources to pay;
- Out-of-character purchasing or spending behavior.

What you can do:

- If you think you're a victim of abuse, don't be afraid or embarrassed to complain. The situation will only become worse if you do nothing.
- Consult with someone you trust, such as another family member, clergyman, bank manager, attorney, etc. You are not alone.
- Know the resources you can turn to, including the Attorney General's office, local police, your bank (if money has been taken from your accounts), and Adult Protective Services.
- Stay connected. Remember, isolation is high risk. Call friends, join groups, visit family.

Abuse by Caretaker:

Risk Factors

- History of substance abuse
- Lack of support from other potential caregivers
- Depression (common among caregivers)
- Sense of little reward in caring for the victim
- Lack of training
- Poor working conditions
- Caregiver belittles or threatens the senior

Trust Your Instincts.

Abusers can be very skilled at persuading you that you are wrong. If you think there is a problem, take steps to stop it. Report it.

- Take control: Look for resources for yourself or others. Sometimes abuse and neglect are the result of enormous stress and isolation.
- If you are a caregiver, make sure you have the resources and support you need to do the job well, and if you know a caretaker, be aware of what they may need to help them through some tough times. There are organizations that provide respite care and other services. Seek out training so that you better understand the issues you are dealing with. Stay connected to friends and family, building a network of support.

VII. Medicaid Fraud Control Unit

The Medicaid Fraud Control Unit is an important part of the Attorney General's office that targets large-scale frauds involving overbilling, kickbacks, substandard drugs and medical equipment, and "Medicaid mills" run by organized criminals. It also safeguards elderly and disabled New Yorkers from abuse and neglect in nursing homes and other health care facilities.

MFCU is the only law enforcement agency in the state specifically tasked with investigating and prosecuting abuse and neglect occurring in residential facilities, such as nursing homes and adult homes, and in hospitals and clinics. In fact, MFCU's jurisdiction extends to all such facilities — regardless of whether the facility receives payments under the Medicaid program or the patient is a Medicaid recipient.

The MFCU has offices across the state. You can find contact information in the Resources at the back of this book.

MFCU's regional offices handle patient abuse and neglect complaints, including those involving the misappropriation of patients' funds. Due to the number of residential care facilities in New York City, MFCU established a special Patient Protection Section, made up of attorneys, investigators and nurse analysts who investigate and prosecute patient abuse and neglect cases in the five boroughs.

Contact Us

If you have questions or would like to make a report to the Medicaid Fraud Control Unit, call the Attorney General's Hotline

1-800-771-7755

Or file a complaint online:

www.ag.ny.gov/comments-mfcu

Bill of Rights for Nursing Home Residents

All residents of nursing homes in New York State have the right to:

- Dignity, respect and a comfortable living environment;
- Quality care and treatment without discrimination;
- Freedom of choice to make your own independent decisions;
- The safeguard of your property and money;
- Safeguards in admission, transfer and discharge;
- Privacy in communications;
- Participate in organizations and activities of your choice;
- An easy to use and responsive complaint procedure;
- Exercise all of your rights without fear of reprisals.

VIII. Take Control of your Finances, Your Health Care

There are legal steps you can take to plan ahead for your finances and your health care. It's a good idea to discuss these with a lawyer, accountant, physician and your family and loved ones.

Power of Attorney

A power of attorney is an important tool in planning for future incapacity or disability resulting from a catastrophic accident, Alzheimer's disease or other serious illness. One person, known as the "principal," appoints one or more individuals, known as "agents," to act on behalf of and represent the interests of the principal.

As the principal, you determine the scope of the power of attorney: it can be limited to an agent signing checks on your behalf, or broad enough to allow the agent to do almost anything you could otherwise do. You can appoint more than one agent to act in different capacities or to make decisions jointly. You can also appoint a monitor who receives a record of all transactions.

An important reason to do this in advance is so that you can choose the person to act as your agent. It should be someone you trust

A Power of Attorney

cannot be used to make medical decisions on your behalf. There are separate legal documents, like a health care proxy, that you must consider and sign to make these designations.

completely and would always act in your best interests. Think about whether the person you are considering as your Agent is good at handling money and making difficult decisions, and whether they can get along with other members of your family. You should also review your choice periodically, particularly if the person you appoint undergoes personal changes or crises, like a divorce, loss of job, or gambling or substance abuse issues.

It's important to remember that this is a designation that should depend as much upon the person's skills as their closeness to you. It is often the case that people we love and trust may not be reliable with finances or well organized even in their personal lives. There are those who at one point in their lives might be ideal agents, but don't have the time or ability to take that on right now. Whoever you consider, make sure you both know what is involved and whether that choice is the best one for all parties.

On the other hand, if someone who has not executed a Power of Attorney becomes incompetent, nobody will be able to access and manage their assets and finances without initiating a court guardianship proceeding. These proceedings tend to be expensive, time consuming and unpleasant, and the person ultimately selected by the court to serve as guardian may not be someone who the individual would have selected. A guardianship proceeding can often be avoided simply by having a Power of Attorney in place.

For More Information

The Attorney General's office produces a booklet entitled "Planning Your Healthcare in Advance". It provides many details about these issues and can be helpful in a planning process and in discussions with family. You will find information about our publications on page 18 in the Resources section.

Advance Care Directives

In New York State, the best way to ensure that your health care wishes are known and followed is to use Advance Directives. These are legal documents that will speak for you if you are unable to speak for yourself.

A Health Care Proxy allows you to appoint someone to make decisions regarding the use of life-prolonging treatment when you are unable to make such decisions. It is in effect only after a physician decides you are not able to make your own decisions.

This covers any time you are unable to make your own medical decisions, not only at the end of life. Without a health care proxy, a doctor may be required to provide you with treatment you may have refused if you were able. No one—not even your spouse—can act on your behalf unless you appoint them using a health care proxy.

Choose a health care agent who you trust and are confident will advocate for your preferred treatment, making sure that your wishes are carried out. You should discuss those wishes with your health care agent. Talk about your values and beliefs. No one can plan for every scenario. The more your agent knows, the easier it will be to make decisions for you.

The Living Will is your personal statement about care you want — or don't want — at the end of life. It is a document that contains your health care wishes and is addressed to unnamed family, friends, hospitals and other health care facilities. It takes effect when you cannot make your own decisions, or are unable to communicate your wishes, and your doctor confirms that you have an incurable, irreversible condition.

New York does not have a statute governing living wills, but the state's highest court has ruled that living wills are valid as long as they provide "clear and convincing" evidence of your wishes.

The Do Not Resuscitate Order (DNR) tells health care providers and emergency workers not to provide life saving treatment if a patient's heart or breathing stops. It takes effect when signed by a doctor. In a hospital, the form is provided, signed by a doctor and kept in the patient's chart. It can follow the patient to another hospital.

Outside of a hospital, a "Nonhospital Order Not to Resuscitate" form produced by the NYS Department of Health is used. It can be kept with the patient in the event of an emergency. You can also include DNR instructions in your Health Care Proxy or Living Will.

The "MOLST "Form

Medical Orders for Life Sustaining Treatment form allows doctors to record your preferences regarding CPR, mechanical intervention and other life sustaining treatments onto one form as a physician order. MOLST is generally for patients with serious health conditions (advanced progressive chronic illness or terminal illness) and others who are interested in further defining their care wishes as they face the end of life.

It must be completed by a health care professional and signed by a New York State licensed physician to be valid.

This form can help centralize and summarize advance directives and end-of-life wishes and. It is not intended to replace your current health care proxy form and/or living will.

Health Care Proxy and Living Will:

There's a difference.

Although the health care proxy and living will are both advance care directives, they are not the same thing. You should consider having both. The living will can be an important tool for your health care agent: it is evidence of your wishes and it can provide your agent with the guidance they may need to make hard decisions.

Resources

Agencies and other organizations where you may find more information.

Office of the New York State Attorney General

www.ag.ny.gov

Hotline: 1-800-771-7755

Executive Offices

The Capitol
Albany, NY12224-0341
(518) 776-2000

28 Liberty Street
New York, NY 10005
(212) 416-8000

Binghamton Regional Office
State Office Building, 17th Floor
44 Hawley Street
Binghamton, NY 13901
Phone: 607-251-2770

Brooklyn Regional Office
55 Hanson Place Suite 1080
Brooklyn, NY 11217
Phone: 718-560-2040

Buffalo Regional Office
Main Place Tower, Suite 300A
350 Main Street
Buffalo, New York 14202
Phone: 716-853-8400
Consumer Frauds: 716-853-8404

Harlem Regional Office
163 West 125th Street, Suite 1324
New York, N.Y. 10027
Phone: 212-364-6010

Nassau Regional Office
200 Old Country Road, Suite 240
Mineola, NY 11501
Phone: 516-248-3302, 516-248-3300
Consumer Frauds: 516-248-3300

Plattsburgh Regional Office
43 Durkee Street, Suite 700
Plattsburgh, NY 12901
Phone: 518-562-3288
Consumer Frauds: 518-562-3282

Poughkeepsie Regional Office
One Civic Center Plaza - Suite 401
Poughkeepsie, NY 12601-3157
Phone: 845-485-3900

Rochester Regional Office
144 Exchange Boulevard
Rochester, NY 14614-2176
Phone: 585-546-7430
Consumer Frauds: 585-327-3240

Syracuse Regional Office
300 South State St
Syracuse, NY 13202
Phone: 315-448-4800
Consumer Frauds: 315-448-4848

Suffolk Regional Office
300 Motor Parkway, Suite 205
Hauppauge, NY 11788
Phone Number: 631-231-2424
Consumer Frauds Number: 631-231-2401

Utica Regional Office
207 Genesee Street
Room 508
Utica, NY 13501
Phone: 315-864-2000

Watertown Regional Office
Dulles State Office Building
317 Washington Street
Watertown, NY 13601
Phone: 315-523-6080

Westchester Regional Office
44 South Broadway
White Plains, New York 10601
Phone: 914-422-8755
Consumer Frauds: 914-422-8755

Medicaid Fraud Control Units

Albany	518- 533-6011
New York City	212-417-5300
Buffalo Regional Office	716- 853-8500
Hauppauge Regional Office	631-952-6400
Pearl River Regional Office	845-732-7500
Rochester Regional Office	585-262-2860
Syracuse Regional Office	315- 423-1104

Publications from the NYS Office of the Attorney General

Public Information and Correspondence
The Capitol
Albany, NY 12224
www.ag.ny.gov/intergov-affairs/publications or Fax: 518-650-9401

Publications are available free of charge; you may also order in quanitity for a group. View and order publications online, or by mail or fax . Here are some you may be interested in:

A Housing Guide for Senior Citizens

This guide addresses key issues involved with owning or renting a home in later years.

Predatory Lending

Issues surrounding borrowing money, particularly for mortgages.

Homeowner Protection Program

Help for Avoiding Foreclosure and rescue scams.

Smart Seniors, Smart Investors

Tips for older adults about making smart investments and avoiding investment fraud.

Fair Housing

Discusses laws concerning discrimination in the rental, sale or financing of homes.

Tenants Rights

An explanation of leases, rent, safety issues, utility services, and tenants' personal protections.

The Patient Protection and Affordable Healthcare Act

Explains how the federal law benefits New Yorkers.

Real Problems with Healthcare

Explains how the Office of the Attorney General's Healthcare Bureau can help New Yorkers.

Residential Care: Protecting Patients from Abuse and Neglect

Planning your Health Care in Advance
Information on advance directives, pain management, hospice care, and organ donation, among other topics.

Health and RX Discount Cards

This brochure gives advice on making smart purchases when considering health discounts.

Protecting Yourself from ID Theft

ID Theft Kit: What to do if You have been Victimized

Straightforward directions on immediate steps to take if your identity is stolen.

Home Improvement Contractor Tip Card

Savvy Consumer

Some tips on making smart purchases.

Other Government Agencies

New York State Department of State
Division of Consumer Protection
Consumer Assistance Unit
99 Washington Avenue
Albany, New York 12231-0001
Consumer Assistance Hotline:
(518) 474-8583 &
(800) 697-1220 (toll free)

NYS Department of Financial Services
877-226-5697
www.dfs.ny.gov

New York State Office for the Aging
2 Empire State Plaza
Albany, New York 12223-1251
Help Line: (800)342-9871
General Assistance: 800-342-9871

U.S. Dept. of Health and Human Services
Administration on Aging
Public Inquiries: (202) 619-0724
Eldercare Locator (to find local resources):
800-677-1116
AoA Fax: 202-357-3555

New York City Office
212-533-6200 Fax: 212-477-4912

Long Island Office
516.420.0500 Fax: 516-420-1095

Mid Hudson Office
914.333.0550 Fax: 914.333.7519

Upstate New York
716-881-5222 or 800-828-5000
Fax: (716)8835349

Better Business Bureau
newyork.bbb.org
upstateny.bbb.org

Credit Reporting Bureaus

Experian
Order a Credit Report and Score: 888-397-3742
Help with Fraud, Identity Theft and Credit:
888-397-3742
www.experian.com

TransUnion:
Purchase TransUnion Credit Report:
800-888-4213
disclosure.transunion.com

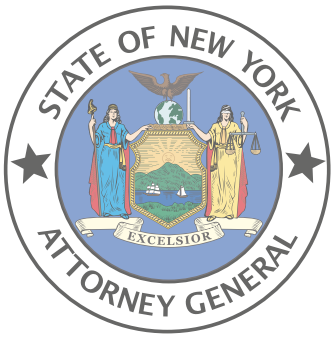
Disputes: 800-916-8800
dispute.transunion.com

Fraud Alert or Security Freeze
Fraud Alert: 800-680-7289
fraud.transunion.com
Security Freeze: 888-909-8872
freeze.transunion.com

Report Fraud or Identity Theft:
TransUnion Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
800-680-7289

Equifax
www.equifax.com/home/en_us
Free credit report: 800-685-1111
www.equifax.com/fcra
Fraud Alert : 888-766-0008

Innovis
www.innovis.com/InnovisWeb/


STATE OF NEW YORK
EXCELSIOR
ATTORNEY GENERAL