DON'T GET SCAMMED, GRANDMA!

Protecting Seniors From Financial Predators

OUR MISSION

Everywhere you turn, there is the possibility of being scammed. The best way to combat the scams circulating around us, is to be informed. Our office recently did a virtual seminar entitled "Don't Get Scammed, Grandma! Protecting Seniors from Financial Predators." We discussed the most common scams, how to spot situations where an individual is susceptible to scams, and legal protections that can be used to protect against scams. We hope this information will help our clients protect themselves and their loved ones.

-Samantha K. Wolfe

WHAT IS ELDER FINANCIAL ABUSE?

Definition:

- The exploitation of an older adult's resources by someone in a position of trust

Examples:

- Unauthorized use of funds or property
- Coercing changes to legal documents (like wills or trusts)
- Theft of valuables

WHY SHOULD SECURE 2.0 MATTER TO YOU?

COGNITIVE DECLINE OR HEALTH ISSUES CAN IMPAIR JUDGMENT

SOCIAL ISOLATION AND RELIANCE ON CAREGIVERS

DESIRE TO TRUST OTHERS OR HELP FAMILY MEMBERS

LIMITED DIGITAL LITERACY (MAKING ONLINE OR PHONE SCAMS MORE EFFECTIVE)

WHAT ARE THE MOST COMMON SCAMS?

Phishing Scams

Tech Support Scams

Romance Scams

Lottery and Sweepstakes Scams

Government Impersonation Scams

Online Shopping or Classified Add Scams

Healthcare or Prescriptions Scams

Family Member Impersonation Scams

Phishing Scams

What It Looks Like:

- Fake emails that appear to be from a reputable company (bank, online service, etc.) asking for personal details or instructing the recipient to click a malicious link.

Why It Works:

- Seniors may be less familiar with detecting scam cues like suspicious URLs or spelling errors.
- Usually, these messages are sent from emails accounts are phone numbers posing as a reliable business (JP Morgan Chase, Bank of America, American Express).

How to Avoid This Scam:

- Practice being extra cautious when opening messages from supposedly reliable sources.
- Banks will **NEVER** ask for bank account information, card information, Social Security Numbers in emails or text messages.
- When in Doubt, call the bank or organization **DIRECTLY** to verify the message you received is legitimate before opening it or doing what they ask.

Tech Support Scams

What It Looks Like:

- A pop-up or unsolicited call claiming the senior's computer has a virus and asking for remote access or payment to "fix" it.

Why It Works:

- Many seniors trust supposed "experts" and fear losing important data if they don't comply.
- Many of the messages impersonate reputable companies such as Microsoft, Apple, and McAfee.

How to Avoid This Scam:

- If you receive a message like this, it is **most likely** a scam.
- **Do not call the number the message provides you,** instead you should call the company they "work for" yourself.
- To find this contact information, google the name of the company and visit their website they will have contact information for their support team.
- When you call, ask if the message you received is legitimate.

Romance Scams

What It Looks Like:

- Scammers create fake profiles on dating sites or social media to build emotional bonds, then request money for emergencies or travel.

Why It Works:

- Emotional vulnerability and the promise of companionship can override caution regarding financial requests.

How to Avoid This Scam:

- Do not send money to anyone you haven't met in person.
- The use of Artificial Intelligence makes it very easy for someone to create videos and audio messages.
- Just because you were sent a video or audio message of them does not mean they're real.

Lottery and Sweepstakes Scams

What It Looks Like:

- Emails or messages stating the senior has “won” a large sum of money or a prize but must pay fees or taxes upfront.

Why It Works:

- The excitement of a big win can lead some to overlook the red flag of having to pay money to claim a prize.
- These individuals impersonate reputable lottery or sweepstakes organizations such as state or local lottery organizations.

How to Avoid This Scam:

- Like with most scams, attempt to contact the organization they are posing as directly by googling the organization **BEFORE** making any sort of payment.
- If you can not find the organizations website it is **MOST LIKELY** a scam.
- Reputable lottery or sweepstakes companies will typically **withhold taxes or fees from the winnings** they won't ask you to pay any of that prior to you receiving the money.
- Note: Taxes are based on an assessment of income, if you have yet to receive the income, you **WILL NOT** be taxed on it; you will never pay taxes prior to receiving funds.

Government Impersonation Scams

What It Looks Like:

- Emails that appear to be from the IRS, Social Security Administration, or other agencies, threatening legal action unless personal information or payment is provided immediately.

Why It Works:

- The threat of arrest or losing benefits can be alarming, prompting hasty, uninformed decisions.

How to Avoid This Scam:

- Do not respond to the email or any of its contents.
- The IRS or other agencies will never ask for personal information over email; any personal information they may require will most likely be given to them via a physical form.
- Government organizations such as the IRS contact you almost exclusively through physical mail.
- If you are still worried by the message, visit the corresponding government website and inquire into the contents of the message you received.

Online Shopping and Classified Ad Scams

What It Looks Like:

- Fake websites or listings offering deep discounts or nonexistent products, then disappearing once payment is made.

Why It Works:

- Seniors may be unfamiliar with verifying secure sites or detecting counterfeit online sellers.

How to Avoid This Scam:

- Never blindly trust sales or discounts you see unless they were given to you on a website you already visited.

Example:

- If you receive an email of a sale do not trust it unless you can verify the sale on a reputable business's website.
- If you are unfamiliar with the business use caution as **when something seems too good to be true, it often is.**

Healthcare and Prescription Scams

What It Looks Like:

- Websites or emails advertising cheap or “miracle cure” prescription drugs requiring an upfront fee or personal details.

Why It Works:

- Health concerns and high medication costs can tempt seniors into believing too-good-to-be-true offers.

How to Avoid This Scam:

- Only use pharmacies or healthcare providers that are licensed and recognized by state or national regulatory bodies.
- Avoid unknown or unverified websites offering significantly discounted medications or “miracle cures.”
- Call your primary care physician and ask about the medication.

Family Impersonation Scams

What It Looks Like:

- Scammers pretend to be a grandchild, niece/nephew, or other relative in distress (e.g., stranded abroad, in jail, or involved in an emergency).
- They often claim to have lost their wallet or phone and urgently need money.
- They use emotional manipulation—fear, guilt, or secrecy—to pressure seniors into sending funds.

Why It Works:

- Seniors may be eager to help loved ones in trouble, especially if there's a perceived risk of harm or embarrassment.
- Emotional pleas can override logic, leading to quick, unverified money transfers.
- Scammers sometimes research personal details from social media to sound convincing.

How to Avoid This Scam:

- Create a safe word or phrase with loved ones that lets you know its really them talking.
- Artificial intelligence can easily be used to spoof someone voice using only a sentence of them speaking.
- Just because it sounds like them doesn't mean it is them.
- If they aren't someone that typically asks you for money like that, it may be a scam.

Behavioral Warning Signs of Financial Abuse

- Sudden fear, anxiety, or confusion about money.
- Unexpected isolation from friends or family.
- Changes in mood or personality related to finances.
- Being secretive with information they would commonly disclose.

Financial Warning Signs of Financial Abuse

- **Large/Unexplained Transactions:** Sudden withdrawals, transfers, or frequent ATM use.
- **Unpaid Bills & Disorganized Records:** Missing statements, overdue payments despite funds.
- **Strange Account Activity:** New signers, wire transfers, unusual charges or checks.
- **Missing Property/Valuables:** Jewelry, collectibles, or cash disappearing.
- **Suspicious Document Changes:** Abrupt shifts in wills, trusts, or beneficiaries.
- **Coercion or Pressure:** Reluctance to discuss finances around certain individuals.

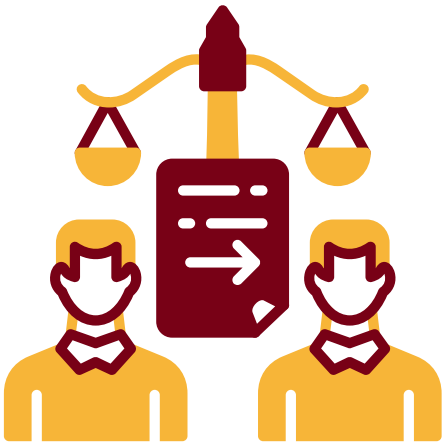
Legal Methods to Protect Our Seniors Finances

- Durable Power of Attorney (POA)
- Guardianships or Conservatorships
- Trusts as a Protective Measure
- Third Party Oversight
- Court Orders
- Preventative Documentation and Planning

Durable Power of Attorney (POA)

Definition:

- A legal document allowing a trusted agent to manage the principal's financial affairs if the principal becomes incapacitated or unable to handle matters.



Key Features:

- Durability: Remains in effect even if the principal loses mental capacity.
- Scope & Limitations: Can be broad or limited to specific transactions.
- Safeguards: Specify reporting requirements or require dual signatures to reduce misuse.

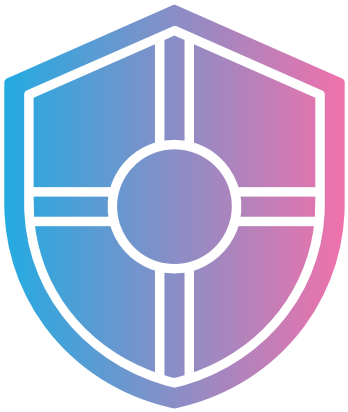
Advantages:

- Avoids costly court proceedings for guardianship.
- Allows seniors to choose someone they trust before incapacity occurs.

Guardianships or Conservatorships

When Used:

- If an older adult lacks the ability—or is otherwise unable—to manage their finances and no valid POA exists (or it's insufficient), the court can appoint a guardian or a conservator. This does not require the individual to be fully incapacitated; it simply acknowledges that they need assistance handling some or all of their affairs.



Court Oversight:

- The appointed guardian/conservator must file regular reports and accountings, ensuring added protection against misuse or exploitation.

Trusts as a Protective Measure

Purpose:

- A trust places assets under the management of a designated trustee, helping shield an older loved one's finances from potential predators or opportunistic relatives. It ensures that funds are managed in line with the senior's best interests.

Revocable Trusts:

- The older adult (grantor) retains control while cognitively able.
- A successor trustee can take over if the grantor becomes incapacitated or falls victim to undue influence.
- Flexible for changing family or financial circumstances.

Irrevocable Trusts:

- Offers stronger asset protection because the trust cannot be easily altered or dissolved by the elderly individual.
- Prevents unscrupulous individuals from freely accessing or manipulating the senior's assets.

Third Party Oversight

Professional Fiduciary or Care Manager:

- Hiring a licensed fiduciary or care manager offers unbiased financial oversight.
- Reduces the likelihood of family disagreements or misuse by relatives.

Co-Trustees or Co-Agents:

- Splitting responsibilities among two or more individuals encourages checks and balances.
- Each party can report suspicious activity, providing greater security for the senior's assets.

Financial Institutions:

- Many banks offer services such as "view-only" access or transaction alerts for authorized third parties.
- Seniors can give a trusted relative or advisor permission to review account activity without the ability to withdraw funds.

Court Orders

Protective Orders:

- A judge can issue an order to freeze financial accounts if there is suspicion of exploitation.
- Prevents the dissipation of assets while investigations or legal actions are pending.

Accountings and Audits:

- Courts can require periodic accountings, compelling guardians, conservators, or fiduciaries to document all transactions.
- Ensures oversight, creating a paper trail that helps identify irregularities early.

Emergency Orders:

- If immediate action is needed to protect a vulnerable senior, courts can grant emergency authority to a caretaker or fiduciary.
- Allows swift intervention to stop ongoing abuse or unauthorized access to funds.

Enforcement and Penalties:

- Courts can impose fines, restitution, or even criminal penalties on individuals found to have exploited a senior.

Protective Documentation and Planning

Advance Health Care Directives:

- Ensures medical decisions align with the senior's financial and personal goals.

Updated Estate Documents:

- Regularly review wills, trusts, and POAs to match current wishes and circumstances.

Clear Communication:

- Having open discussions and written instructions about asset management can deter would-be abusers.

Commonly Asked Questions

What steps can I take if I suspect abuse?

Immediate Actions:

- Speak with the senior privately to gather more info.
- Notify financial institutions to place holds or alerts on accounts.
- Contact Adult Protective Services (APS) to file a report.
- Consult an attorney about legal measures (e.g., POA, guardianship).

Key Point: Early intervention often prevents further losses.

What If my loved one doesn't want help?

Respect for Autonomy:
- Recognize the senior's right to make personal choices—even risky ones.

Encourage Transparency:
- Offer to review accounts together or set up transaction alerts.
- Emphasize the value of a "backup plan" in case of emergency.

Potential Legal Avenues:
- If safety is at risk, explore court intervention (guardianship, conservatorship) with professional advice.

Bottom Line:
- Balancing respect for independence with protective steps can be challenging—seek guidance early.

When should I seek Court Intervention?

No Valid POA or Trust in Place:
- Senior needs help managing finances but can't (or won't) designate an agent.

Ongoing Exploitation:
- Evidence of fraud or theft by caregivers or family members.

Immediate Risk:
- Urgent need to freeze accounts or safeguard assets.

Court Oversight:
- Guardianships/conservatorships provide structured monitoring but can be costly or perceived as intrusive.

Remember:
- Court intervention is usually a last resort but can be necessary to halt serious abuse.

Can Banks or Other Institutions Help Me?

Bank Safeguards:

- Many offer “trusted contact” designations or can temporarily freeze suspicious transactions.

Financial Advisors:

- Can flag unusual activity and recommend protective measures.

Reporting Suspected Abuse:

- Institutions can alert Adult Protection Services (APS) or law enforcement if they suspect criminal activity.

Tip:

- Encourage seniors to maintain open communication with their financial institution and advisors.

Next Steps

Call (717) 655-2676 to schedule an initial consultation

Thank you for reading!

THE LAW OFFICES OF
SAMANTHA K. WOLFE
LLC
Providing mindful legal direction

20 East Sixth Street, Suite 206,
Waynesboro, PA 17268
Monday through Friday 8:30 am to 4:30 pm

717-655-2676
skwlawoffice.com
@skwlawoffice
The Law Offices of Samantha K. Wolfe, LLC
@skwlawoffice
The Law Offices of Samantha K. Wolfe, LLC

TEAM INTEGRITY	CONSULTATIONS	SOCIAL MEDIA
We uphold the highest standard of honesty in all our actions.	Contact Us Today For A Consultation	Follow Us on Social Media