

How To Prevent Elder Financial Abuse

CANHR is a private, nonprofit 501(c)(3) organization dedicated to improving the quality of care and the quality of life for long term care consumers in California.

Plan Ahead – Be Pro Active:

- Create a Durable Power of Attorney for property.
- Create an estate plan or update your existing one.
- Put all financial instructions in writing.
- Keep records of all financial transactions and legal documents up to date and in a safe place. Be sure to let your designated agent know where these documents are located.
- Appoint a trusted financial advocate to serve as an extra set of eyes in guarding against financial abuse.

Practice Preventive Banking:

- Use direct deposits.
- Keep checks in a safe place and never sign a blank check allowing someone else to fill in the amount.
- Never give someone your ATM, credit card PIN or Social Security number.
- Be cautious with joint accounts because all parties on the account have equal access to the money.
- Always take time to check your bank statements carefully for unauthorized withdrawals. When in doubt, contact the bank immediately to stop payment on checks, to flag or to put a hold on the account or to close an account.
- Work with your bank to set up a suspicious activity alert to notify you and your trusted financial advocates.

Establish Relationships with Legal and Financial Professionals:

- Communicate on a regular basis with your banker, attorney and/or financial advisor. They can help detect changes or unusual activities that might signal problems.
- Make sure that they understand your current and future financial needs and wishes.
- If you need help paying bills, consider automatic billing paying services through a bank or hiring a bonded professional fiduciary. If there is someone helping with personal finances or bill paying, ask a trusted friend or professional to regularly review your bank and other financial statements.

- Never allow a non-attorney to change your living trust, will, or durable powers of attorney.
- Periodically check with your county registrar to review your property title to make sure there are no liens or encumbrances.

Be Cautious about Signing Powers of Attorney:

- Before signing a power of attorney for a bank account, general purposes or for financial management, make sure you know well and absolutely trust the person whom you are naming as your agent.
- Make sure you have known the person for an adequate period of time and that you are comfortable with that person's ability and commitment to carry out your exact wishes in the future.
- Be aware that a power of attorney is a powerful legal document that can sometimes be used by unscrupulous persons to legally have access to your money and assets. Consult an attorney or make an appointment with legal services before executing a power of attorney.

Check Health Care Billing:

- Question bills or notices for services that you do not understand.
- Report providers and companies that have suspicious billing practices to the Department of Consumer Affairs (dca.ca.gov).
- Never give your social security number, Medicare or Medi-Cal number to unauthorized providers or anyone offering "free" health care services or equipment.

Be Aware of Telephone & Mail Solicitations:

- Hang up on phone solicitations. The telephone is the gateway to financial elder abuse.
- Throw away mail solicitations. You didn't win so don't even bother to say no!
- Just say NO! to any and all prize offers, travel packages, get-rich-quick opportunities, high interest investments, and pleas from unknown people, companies, and charitable or religious organizations.
- Never give your social security number, credit card number, or any personal information over the phone to anyone who calls you.
- Imposters are contacting seniors pretending to be relatives who are stranded, have had accidents or are in trouble with the law and desperate need emergency cash. Never wire or transfer money to "bail out a relative in trouble".

Be Aware of Fake Mobile Apps

- Fake mobile apps are Android or iOS applications that mimic the look and/or functionality of legitimate applications to trick unsuspecting users to install them.
- Once downloaded and installed, the applications perform a variety of malicious actions. Some fake applications are built to aggressively display advertisements to rake in ad revenue, other apps are designed to harvest credentials, intercept sensitive data, divert revenue or infect devices.

Be Aware of E-Signature Scams

Cybercriminals are stealing seniors' financial information and personal identities personal.

- If you receive an unsolicited email telling you that you have a document to sign do not sign it.
- Do not respond to emails from individuals or companies you do not recognize.
- Request hard copies of what you sign whenever you use an e-signature

Avoid Financial Product Salespeople Who Target Seniors:

- Do not attend free lunch and dinner financial seminars. They will have your contact information and follow up to sell you their products or services. The “free luncheon” is the gateway to financial abuse.
- Be wary of “experts” who charge money to pre-qualify or “guarantee” eligibility for government benefits. Seek assistance from a licensed elder estate planning attorney. (Contact CANHR’s Lawyer Referral Services: www.canhr.org/LRS/index.html)