sifma

SENIOR INVESTOR PROTECTION FREQUENTLY ASKED QUESTIONS

ELDER FINANCIAL EXPLOITATION

Defining Elder Financial Exploitation:

The National Center on Elder Abuse defines Financial Exploitation as the illegal or improper use of a vulnerable adult's funds, property or assets. Financial exploitation crosses racial, ethnic and economic lines.

Who Commits Elder Financial Exploitation?

Most cases of elder financial exploitation are committed by a trusted person, family member, caregiver or professional advisor of the client. In studies conducted with older adults, family members were the most common perpetrators of financial exploitation of older adults, followed by friends, neighbors and home-care aides.

What Are Common Examples of Financial Exploitation?

- Taking, misusing or using, without knowledge or permission, money or property from an elder person.
- Forging or forcing an elder person's signature.
- Getting an elder person to sign a deed, will, contract or power of attorney through deception, coercion or undue influence.
- Providing misleading information that influences the elder person's use or assignment of assets.
- Influencing an elder client with diminished capacity to change beneficiaries.
- Improperly using authority provided by a trust or power of attorney.
- Denying elder client with access to their money or preventing them from controlling their assets.

Who commits elder financial exploitation?

Most cases of elder financial exploitation are committed by a trusted person, family member, caregiver or professional advisor of the client. In studies conducted with older adults, family members were the most common perpetrators of financial exploitation of older adults, followed by friends, neighbors and home-care aides.

What are Common Examples of Elder Financial Exploitation?

- Taking, misusing or using, without knowledge or permission, money or property from an elder person.
- Forging or forcing an elder person's signature.
- Getting an elder person to sign a deed, will, contract or power of attorney through deception, coercion or undue influence.
- Providing misleading information that influences the elder person's use or assignment of assets.
- Influencing an elder client with diminished capacity to change beneficiaries.
- Improperly using authority provided by a trust or power of attorney.
- Denying elder client with access to their money or preventing them from controlling their assets.

What Are Common Examples of Financial Scams?

- **Lottery Scam:** Arguably one of the most common and successful scams. Fraudsters call seniors telling them that they have won a large sum of money, and all they need to do to collect their prize is pay upfront processing fees or taxes. The caller begins in a friendly manner, although over time the calls may become threatening and the collection tactics aggressive.
- **Sweetheart / Romance Scam:** An internet based scam that uses fake profiles on dating sites and in social media to target victims, establish a romantic relationship, and then make pleas for financial assistance to drain the resources of the smitten victim. If successful, this scam may progress into outright blackmail, knowing that the victim does not want public knowledge of their actions.
- **Foreign Letter Fraud:** The recipient of the letter or e-mail is given the "opportunity" to share in a percentage of the money that the sender is trying to get out of their country. The recipient is encouraged to send tax money and/or his or her bank information for ease of transfer.
- **Grandparent Scam:** A senior receives a phone call from someone claiming to be their grandchild who is in desperate need of money and unable to approach their parents. The scammers often rely on social information found on social media to defraud the seniors and tend to strike during school breaks.
- **Affinity Scam:** Where a fraudster claims to be a member of the same ethnic, religious, career or community-based group to gain the target's trust.

What Can I Do If I Suspect Elder Financial Exploitation?

First, escalate your concern to the appropriate point of contact within your firm and develop a plan. Then determine if a Power of Attorney has been designated. If so, contact the named agent and address your concerns. During future meetings, review current information with your client to determine any changes in transaction patterns, large or frequent withdrawals, changes to beneficiaries, Power of Attorney or trusted contacts.

COGNITIVE DECLINE

Defining Cognitive Decline:

Cognitive decline generally refers to age-related changes in the brain. This is broader than any diagnosed impairment, and refers to a general decline in executive function, processing speed and other related cognitive abilities. The rate of cognitive decline varies by individual, sometimes occurring from middle-age onwards, and sometimes occurring much later. Even otherwise high-functioning, healthy adults can be vulnerable to exploitation due to some level of cognitive decline.

Why Are Mature Investors Often Targeted in Scams?

Though anyone can fall victim to a scam, mature investors are often targeted because of a variety of factors, including: large available cash flow; embarrassment of feeling less capable; instilled values of respect and trust for professionals; and varying levels of cognitive function.

What Can I Do If I Suspect Cognitive Decline?

First, escalate your concern to the appropriate point of contact within your firm and develop a plan. Then determine if a Power of Attorney has been designated. If so, contact the named agent and address your concerns. Request client authorization to speak with a family member or friend and suggest they include this individual in future meetings. Lastly, send a letter to the client outlining discussions and decisions made during meetings.

UNDUE INFLUENCE

Defining Undue Influence:

Undue influence is when a person in a position of trust coerces a vulnerable adult into giving away or loaning money or property, either directly, or through a trust, marriage, inheritance or adoption.

How do Perpetrators Use Undue Influence?

- **Dependence:** By promising the client they will take care of them for the rest of their lives.
- **Fear or Vulnerability:** By lying to the client suggesting no one else cares for them. This can include suggesting that trusted friends, advisors and family members are trying to steal their money.
- **Isolated Environment:** By detaching the client from social contact with other family members, advisors, friends and society. This can include moving to a new area, preventing phone calls, intercepting mail and preventing participation in social groups.
- **Restricted Freedom:** By convincing the client they will lose their house and be placed in a nursing home.
- **Intimidation:** By threatening the client with harm, neglect or abandonment if they don't agree to do what they are told.
- **Medication:** By over- or under-medicating the client so they become weak, dependent and compliant.

PREVENTION AND NEXT STEPS

How Can We Help Protect Ourselves, Our Clients and Our Loved Ones Against Financial Exploitation and Scams?

- **Investigate Before Investing:** Urge loved ones to take the time to research any investment – read relevant materials, and ask for unbiased references.
- Understand Undue Influence: Many mature investors become vulnerable with age. Review how perpetrators use undue influence and set up plans to defend against them.
- Understand Cognitive Decline: The latest research shows that even high-functioning senior professionals can still be vulnerable to scams. Reduce risks later in life by creating a plan early to identify powers of attorney, trusted contact authorization forms and advance directives.
- Be Wary of Unsolicited Offers: Thieves use email, faxes and internet postings to create a buying frenzy to boost the share price of thinly traded stocks. Once they quit promoting the company, the share price quickly falls. If the victim sends money abroad and something goes wrong, the funds are nearly impossible to recover.
- Protect Personal Information:
  - > Shred any documents that contain personal information, such bank or credit card statements, when you no longer need them.
  - > Do not carry your Social Security card in your purse or wallet. Do not have this number printed on your checks.
  - > Even if the caller seems harmless, do not give out any personal information over the phone.
  - > Make sure your computer is running current firewall or malware detection software – thieves can use links in unsolicited emails to obtain your financial information.
  - > Stay alert for warning signs with those close to you, such as family members, friends or neighbors.
  - > Get a free copy of your credit report annually from one of the major credit reporting agencies: Equifax, Experian or TransUnion, and review for inaccurate information or unrecognized entries.

What Should We Do if We Fall Victim to a Scam or Other Fraudulent Activity?

First, immediately place a fraud alert on your credit report and notify the appropriate banks, brokerage firms and credit card companies to report the fraud and help prevent future fraud activity. Then begin to gather and document all conversations and/or correspondence you have had with regard to the theft. Also contact the local authorities and share any documentation you have collected. Depending on the type of activity, also file a complaint with the Federal Trade Commission (FTC); US Postal Service or the Social Security Administration.