TESTIMONY OF

HOWARD M. SILVERSTONE, MBE, CPA, CFF, FCA, CFE

MEMBER OF THE AMERICAN INSTITUTE OF CPAs FORENSIC AND LITIGATION SERVICES (FLS) FRAUD TASK FORCE

BEFORE THE

ERISA ADVISORY COUNCIL ON

EMPLOYEE WELFARE AND PENSION BENEFIT PLANS

October 2020

I am pleased to appear before the Advisory Council on behalf of the American Institute of Certified Public Accountants (AICPA) to discuss considerations for recognizing and addressing participants with diminished capacity. I have provided materials to the Advisory Council in advance of today's hearing, which are included as Appendix A to this testimony. Those materials include copies of the AICPA Forensic and Valuation Section (FVS) Eye on Fraud publications: Elder Financial Abuse Trends; Cyberfraud- Current Issues and Trends; Investment Fraud; and a Consumer Fraud Risk Framework.

Financial Abuse Trends

Addressing those with diminished capacity, the elderly and other vulnerable members of the population

The U.S. Securities and Exchange Commission has recognized that a diminished mental capacity can impair a person's ability to make appropriate financial decisions.[1] Similarly, the SEC

[1] https://www.investor.gov/additional-resources/information/seniors/diminished-capacity

recognizes that older people can be targets for financial abuse.[2] In their joint "Consumer Advisory and Investor Bulletin", June 2015, the Consumer Financial Protection Bureau and the SEC noted, "diminished financial capacity is a term used to describe a decline in a person's ability to manage money and financial assets to serve his or her best interests, including the ability to understand the consequence of investment decisions."[3]

As a Certified Public Accountant, with almost 40 years of experience in accounting, including over 35 years as a forensic accountant, I know that anyone can be a victim of fraud at any given time. However, in the 21st century, with a continually changing and evolving technology landscape, I believe those who are older and/or with a diminished mental capacity face a more difficult challenge than other members of the general population.

I have made many presentations to various groups on this subject and one of the daunting statistics is that the Population Reference Bureau ("PRB") estimates the number of Americans aged 65 and older is projected to almost double from 52 million in 2018 to 95 million by 2060.[4] At the same time, the PRB estimates that those suffering from Alzheimer's disease could reach 13.8 million in 2050 from 5.8 million in 2018.[5] These two groups are not mutually inclusive however. Age is not necessarily the factor in people having a diminished capacity, although it is a factor.

Elder Fraud has been defined as "an act targeting older adults in which attempts are made to deceive with promises of goods, services or financial benefits that do not exist, were never intended to be provided, or were misrepresented."[6] This definition applies across the board where the word "older" could be replaced by "compromised" or indeed "any" and we simply remove the word "Elder" from "Elder Fraud." While the fraud itself may not be different, it is the target who changes and may become the victim because of their mental capacity and their inability to recognize the danger.

In the financial and fraud prevention profession, we are constantly aware of employees, management, vendors, suppliers, competitors and others and their ability to commit fraud. For adults with any kind of diminished capacity, this population of potential perpetrators of fraud can

[2] https://www.investor.gov/additional-resources/information/seniors/elder-fraud
[3] https://files.consumerfinance.gov/f/201505_cfpb_consumer-advisory-and-investor-bulletin-planning-for-diminished-capacity-and-illness.pdf
[4] https://www.prb.org/aging-unitedstates-fact-sheet/
[5] ibid
[6] STOPFRAUD.gov website

include family members, care providers, telephone scammers and others through bank account manipulation, sale of fraudulent products, investment schemes, mortgage scams and others.

Although this abuse can take many forms, financial abuse and exploitation involves the misuse or withholding of an adult's resources, also referred to as material abuse.

It is estimated that 10% of elderly people in North America have already been victims of financial abuse with total reported yearly financial losses of over $2.9 billion. Although the statistics vary between studies and geographic regions in North America, one thing which is consistent is that this is a serious problem and that it is increasing. Awareness is often the first step in combating these types of crimes.

This paper has been written while we are still under the grip of the Covid pandemic. While we do not have any statistics yet on how it has exacerbated the problem, the pandemic has certainly led to increased isolation of the elderly and many others, and the internet has been one of their few windows to the outside world.

I have attached to this paper, a document called "Consumer Fraud Risk Framework." This is a document I have been working on this year with members of the American Institute of CPAs Forensic and Litigation Services (FLS) Fraud Task Force. This framework identifies what we believe is the population of fraud that is perpetrated against consumers. What is most striking about this document is that while we attempted to classify frauds into "buckets", the individual schemes are interchangeable. This means any one or combination of such schemes could be perpetrated against the general population. Examining this vast list of schemes merely amplifies the problem at hand when we consider those who are elderly and/or with a diminished capacity.

I would like to focus on some fraud schemes that have been specifically identified as targeting seniors. But I would like to emphasize these are schemes that essentially target anyone with a diminished capacity and the inability to recognize the immediate danger. The National Council for Aging has identified the top 10 financial scams targeting seniors:

1. Medicare/health insurance scams
    - In certain cases, perpetrators pose as Medicare agents to solicit personal information, which is then used to bill Medicare and pocket the funds.
2. Telemarketing scams

- This is the most common scheme that the elderly face; these schemes are impersonal and have no paper trail and can include fake charities or the pretense that the person calling is from a bank or the IRS and seeking personal information such as bank account numbers, social security numbers and other personal data.

3. Internet fraud
    - Bogus virus scanning software, malicious emails and other phishing scams are among the most popular targeted at senior citizens. Similar to telemarketing scams, these emails will appear to be legitimate and ask for personal information to "verify" an account or transaction.
4. Investment schemes
    - While seniors may have the intention of protecting their savings for retirement, scammers have other ideas. In all-too-familiar schemes, seniors are targeted for schemes, which claim they can get better returns than the market.
    - Types of investment schemes are quite varied and often employ sophisticated devices to "trick" the elder into parting with equity in homes or retirement savings.
5. Homeowner/reverse mortgage scams
    - These include bogus letters that claim to help seniors reduce their property taxes "for a fee" and scammers capitalizing on the reverse mortgage boom, where seniors give up the title to their home in exchange for cash or another property, neither of which crystalize.
6. Counterfeit prescription drugs
    - This is largely an internet-based scam, whereby seniors try to find better pricing than their local pharmacy. This poses a double threat – loss of funds and potential health risks from unsafe drugs.
7. Funeral and cemetery scams
    - Scammers will scan obituaries and prey on a grieving spouse, in some cases claiming the deceased owed them money. In other cases, unscrupulous funeral homes have added unnecessary charges or up-charged for certain expenses.
8. Fraudulent anti-aging products
    - Bogus Botox treatments, homeopathic remedies and others are top of the list for supposed "remedies" aimed at those wishing to conceal their age and feel younger.

-

9. Sweepstakes and lottery scams
    - Request for a payment to "unlock" a prize that the senior supposedly won – the senior receives a check, which they deposit, only to find out days later, bounced, while their payment and the perpetrator have both disappeared.
10. The Grandparent scam
    - This involves a call whereby the scammer will ask the senior citizen to guess which grandchild is on the phone, thus having the senior divulge a grandchild's name. They will then ask for money in the form of a moneygram or similar payment.

The AARP ("American Association of Retired Persons") suggests that people over 50 years of age are easier targets for such abuse as many are less knowledgeable about the complexities of scams, as well as not knowing their rights, have a tendency to be more trusting and expect everyone to be honest and are more likely to be home than younger people and therefore a better target for telemarketers.

I discussed the specific topic of elder fraud with Amy Nofziger, Regional Director of the AARP Foundation and who works with the AARP Fraud Watch Network and Mark Bagley, head of AARP's Media Relations. They identified IRS scams, tech support scams, grandparent scams and government grant scams as those on the top of AARP's watch list.

Ms. Nofziger said that the IRS scam, whereby the caller claims to be with the IRS and seeks out personal information in order to process a bogus refund or adjust the person's tax return, is "one of the biggest scams and had the most complaints directed towards AARP's Fraud Watch Network."

While acknowledging that tech support scams affect everyone from 18 to 99 years of age, they said that the elderly are at a higher risk, due to the perpetrator's exploitation of the lack of understanding of technical computer issues and trusting someone who claims to be able to assist them.

Ms. Nofziger also said the grandparent scams are among the most egregious as they prey on an elderly person's emotions and family ties. The perpetrator will usually say, "please don't tell mom or dad, I don't want them to know I am in trouble." Many of these scams originate from perpetrators obtaining information from the person's unsecured Facebook page.

We also discussed Government grant scams, which the AARP recognizes is an issue in a Presidential election year such as this. The unwitting victim is told that the government under the outgoing President, has money to spend and award to members of the public. Victims are then asked to provide personal information, such as social security numbers, bank account information and other data, which the perpetrator then uses for fraudulent purposes.

Elder financial abuse often occurs within the family by adult children, or grandchildren, but elder fraud and abuse can also be perpetrated by anyone else who is in a position of power, trust or authority. This can include relatives, friends, neighbors, paid caregivers, landlords, and even financial advisors.

The elderly and those with a diminished capacity are often unable to understand what is happening to them due to advanced age or medical conditions. They may also not be familiar with financial matters, or they could be lonely and isolated, which also makes them more susceptible to becoming a victim of financial abuse. It is, therefore, critical to recognize the possible signs of such financial abuse and understand current reporting options and resources available to help investigate and prevent these crimes from occurring.

Potential Signs of Financial Abuse:

There are many indicators of potential financial abuse, including those listed below. Although many of the indicators of potential financial abuse may be associated with other factors including onset dementia, if there is any reason to suspect that someone is possibly a victim of such financial abuse fraud, they need help. Some of the indicators include:

- Unpaid bills;
- Sudden change in lifestyle;
- Forged signatures;
- Sudden accrual of debts;
- Sudden sale or change in title of home, land, or assets;
- Unexplained transfer of funds;
- Power of Attorney or Wills changed under unusual circumstances;
- Sudden changes in withdrawal amounts;
- Elder complains about missing money or assets;

- Elder reports financial abuse.

As noted above, while some reports by elders may be a part of their dementia or illness, it is recommended that any such indicators be followed up to the extent they have substance to them.

Countering the Problem

AARP's Amy Nofzinger stated what may be obvious to many of us, but needs to be reinforced regularly; "it is crucial people stay aware of current frauds and scams." She added that falling for these scams is not necessarily linked to a person's education level, but depends on their level of vulnerability. However, it is up to relatives and those with financial expertise, such as CPAs, and for groups such as the SEC, CFPB, AARP and others to continually educate and inform elderly family members and clients, or clients with elderly family members. Just like all frauds, understanding the red flags and conducting due diligence is key. Ms. Nofinger's experience with AARP is that a person's financial capability and decision-making are most susceptible to brain changes, which is why it is key for a close family member or financial advisor to stay in touch and closely monitor them.

Safety – The first consideration for any suspected financial abuse is the safety of the person who is the target. If there are visible signs of abuse or there is concern that the person may be in danger, then the incident should be reported to the local law enforcement agency.

Rapport - Developing a rapport with the victim is very important as they may be reluctant to talk about it. In some situations, they may have been relying on and trusting the abuser for assistance with daily activities including cooking and cleaning, and do not have any other source of assistance. It takes time to build a bond with the victim and be respectful.

Documentation - As with any allegation of fraud, documentation needs to be gathered, including bank statements, receipts, bills, power of attorney, wills and any other documents which may be required to provide to authorities.

Take Notes – Write down anything that the victim has said regarding events that have taken place as it often assists with any follow-up which may be required at a later time. In some situations, there may be others that have been victimized or other people that may have been involved.

In their joint bulletin referenced earlier in this paper, the CFPB and SEC recognized the importance of organizing important documents, keeping them in a safe place and readily accessible in an emergency. These include, bank and brokerage statements, mortgage and credit information, insurance policies, pension and retirement benefit summaries, social security payment information and contact information for professionals such as doctors and lawyers.

Ongoing Education/Further Recommendations

While many government and other agencies, such as the SEC, CFPB, AARP and others regularly issue bulletins and updates on this subject, continued education, training and overall awareness are keys to understanding these schemes and assisting the general population in fighting such scams.

The suggestions I make to financial professionals and others include:

- Learn about current identity theft schemes
- Learn about current internet-based fraud schemes
- Learn about current investment fraud schemes
- Identify government and private resources for victims of fraud
- Learn about fraud indicators and warning signs

Specifically, below are some areas where I believe the Department of Labor can assist in the effort:

- Work with, and seek continued input and assistance from, professional accounting organizations, such as the AICPA, State CPA societies, to name a few, as they are aware of the new challenges.
- Commit resources among interested organizations to provide an expedited exchange of knowledge.
- Provide the general public with continued education and warnings through the resources available, including the Social Security Administration and other departments and organizations with access to the vulnerable.
- Establish an ongoing task force, routinely identifying new threats and acknowledging achievements.
- Use various kinds of media resources to reach out to potential victims – many are not internet savvy, so continued messages on and about the dangers are vital.

- Continue to seek the advice and experience of financial and fraud professionals; as noted earlier, professional organizations have a wealth of knowledge and are willing to advise and participate in your initiatives.

Resources

There are many resources available that address fraud against the elderly and those with diminished capacity, and provide useful information related to fraud schemes.

AARP (American Association of Retired Persons) at www.aarp.org has a wealth of information, especially through its Fraud Watch Network http://www.aarp.org/money/scams-fraud. The AARP also sends out press releases through its Fraud Watch Network, including recent issues related to use of public wifi networks, its annual "shred fest" to help avoid identity theft risks, IRS imposter scams and its recent initiative with Frank Abagnale to avoid tech support scams.

The **Financial Fraud Enforcement Task Force** was established in November 2009 to investigate and prosecute financial frauds. This task force also addresses elder fraud and financial exploitation - https://www.stopfraud.gov/protect-yourself.html.

The **Department of Justice** also has an Elder Justice Initiative, which can be found at: https://www.justice.gov/elderjustice.

The **FBI** also addresses fraud against seniors at: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/seniors.

The **National Committee for the Prevention of Elder Abuse** is also dedicated to many issues involving seniors, including those related to financial exploitation. Their information can be found at: http://www.preventelderabuse.org.

The **National Crime Prevention Council** is another resource, which has information related to crimes against seniors: http://www.ncpc.org/topics/crime-against-seniors.

The **National Council on Aging** also addresses financial scams targeting seniors, which can be found at: https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/.

Federal Trade Commission ("FTC") Tip Line also collects information on issues such as identity theft at: https://www.ftc.gov/contact

National Adult Protective Services Association -
https://www.sec.gov/investor/seniors/diminishedcapacity.pdf

The **Securities and Exchange Commission** ("SEC") has published several public education alerts and bulletins on the topic of elder financial fraud including this short article highlighting five red flag warning signs. https://www.sec.gov/oiea/investor-alerts-bulletins/ia_fraud5redflags.html

In 2013, seven federal agencies issued joint guidance in the area of investment schemes targeting the elder population. The press release can be found at: https://www.sec.gov/news/press/2013/elder-abuse-guidance.pdf