



Addressing Elder Financial Abuse

Compliance Webinar 2022



Disclaimer

The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.

No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

“Addressing Elder Financial Abuse” discussed in this presentation is the current version with effective date of November 17, 2022.

The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.



What to expect

Warning signs of elder financial abuse

Some of the most common scams aimed at elders

What to look for when interacting with members and some real examples

The role of your credit union in abuse prevention and reporting

Resources for your team

Definition

Elder Financial Exploitation:

No individual, including a caregiver or fiduciary, may:

Use the resources of a senior citizen for monetary or personal benefit, profit or gain; or

Deprive a senior citizen of rightful access to or use of benefits, resources, belongings, or assets.

Impact

Many older adults that are near, or at, retirement age lack adequate savings and the ability to withstand the financial shock of a scam.

Four in ten late baby boomers (currently ages 51 to 59) are reaching retirement with limited or no savings and are projected to face a savings shortfall.



Exploitation by a Stranger - Scam

Charlie, 82, received a phone call from a “sheriff” in New Orleans. He said Charlie’s grandson had been arrested for intoxication. To be released, the sheriff said that someone needed to pay the grandson’s fine and that his parents were not home. The sheriff told Charlie to wire money to an online address. After the money was delivered, Charlie got a call from someone he thought was his grandson saying that he needed money to get home from New Orleans. Charlie became suspicious when he asked the person claiming to be his grandson a few personal questions that he couldn’t answer. The call ended amicably. Then Charlie called a nearby Federal Bureau of Investigation field office to report the incident and filed a complaint with the FBI’s Internet Crime Complaint Center online.

www.justice.gov



Warning Signs of Member Activity

- Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds
- Inconsistent debit transactions
- Uncharacteristic attempts to wire large sums of money
- Closing of CDs or accounts without regard for penalties
- Far-fetched explanations of why money is needed or was spent



Warning Signs of Member Activity

- Abrupt changes in a will or other financial documents
- Unexplained disappearance of funds or valuable possessions
- Discovery of an elder's signature being forged for financial transactions or for the titles of his/her possessions
- Sudden appearance of previously uninvolved relatives claiming their rights to an elder's property or possessions

Question One

Who is the most likely to commit elder financial abuse?

- A. Financial institution employees
- B. Random strangers
- C. Nursing home employees
- D. A relative or trusted caregiver

Warning Signs of Member Activity

- Complaints of (or confusion about) stolen or misplaced credit/debit cards or checkbooks
- Frequent large withdrawals, including daily maximum currency withdrawals from an ATM
- Opening new joint accounts
- Sudden non-sufficient funds activity



Exploitation by a Family Member

Joseph and Malvina, both 80 and retired, had taken in their daughter after her release from prison. Soon after she moved in, the couple received one credit card bill for \$8,347, another for \$12,694, and a third for \$10,012. The couple had no idea their daughter had used their credit cards or that she had opened additional credit card accounts in her mother's name. Now, Joseph and Malvina were faced with significant debt. The couple's other adult child contacted Adult Protective Services (APS), the credit card company and the Federal Trade Commission (FTC).

www.justice.gov

2021 Crimes by Type – Victim Over 60



Tech Support -13,900

Non-payment/Non-delivery – 13,220

Identity Theft – 8,902

Confidence Fraud/Romance – 7,658

Personal Data Breach – 6,189

Extortion – 5,987

2021 Crimes by Type – Victim Over 60

Confidence Fraud/Romance – \$432,081,901

Investment – \$277,547,598

Tech Support - \$237,931,278

Personal Data Breach – \$103,688,489

Government Impersonation - \$69,186,858

Identity Theft – \$59,022,153

2021 Elder Fraud Report – FBI and IC3

Exploitation by a Rep Payee

Carollee appeared to take good care of the older adults, including veterans, who lived in the group home where she worked. Because most of the residents were disabled and had no family to represent them, Carollee became the representative payee for their Social Security and Veteran's Benefits. The regular postal carrier became curious when he started delivering over 30 envelopes from Social Security and Veteran's Benefits to Carollee's home each month. He thought she lived alone so he notified the local postal inspector through the US Postal Inspection Service hotline, Veterans Affairs, and Adult Protective Services (APS).

www.justice.gov

What to Look for in Interactions

- The appearance of a new caregiver or “friend”.
- A caregiver or other individual shows excessive interest in the elder's finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations;
- The elder shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;
- The financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her;

Question Two

In 2021 what type of internet scam caused the greatest loss to victims over 60?

- A. Confidence Fraud/Romance
- B. Gambling
- C. Phishing
- D. Credit Card Fraud

What to Look for in Interactions

- A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation;
- The customer moves away from existing relationships and toward new associations with other "friends" or strangers;
- Abrupt changes in a will or other financial documents or transfer of the person's assets to a family member, acquaintance, or care provider without a reasonable explanation;
- The elderly customer lacks knowledge about his or her financial status or shows a sudden reluctance to discuss financial matters.

Exploitation by a Stranger – Lottery Scam

Armando, 78, was thrilled when someone from the lottery called to confirm he had won \$10,000. The person on the phone said that they would send the money after Armando sent a winner's fee of \$500. Thinking only about what he would do with the winnings, he wired the \$500 “winner’s fee” to the address the caller provided. Because he did not receive the promised lottery winnings after a month, he contacted the Federal Trade Commission (FTC).



www.justice.gov

Reporting and Training

Changes to federal law in 2018 requires that credit unions provide appropriate training for all staff and officers who:

- ✓ serve as a supervisory or in a compliance or legal function,
- ✓ may come into contact with a senior citizen as a regular part of their professional duties, or
- ✓ may review or approve the financial documents, records, or transactions of a senior citizen in connection with providing the senior member credit union services.

Reporting and Training

The training must be appropriate to the job responsibilities of each attendee and include:

- ✓ Instructions on how to identify and report the suspected exploitation of a senior citizen internally, and, as appropriate, to government agencies (such as Adult Protective Services) and law enforcement authorities,
- ✓ Common signs and red flags that may indicate financial abuse of older members, and
- ✓ A discussion on the need to protect the privacy and respect the integrity of your members.

Reporting and Training - Immunity

Immunity for individuals

An individual who has received training shall not be liable, including in any civil or administrative proceeding, for disclosing the suspected exploitation of a senior citizen to a covered agency if the individual, at the time of the disclosure- served as a supervisor or in a compliance or legal function (including as a Bank Secrecy Act officer) or was affiliated or associated with, a covered financial institution; and made the disclosure in good faith and with reasonable care.

Reporting and Training - Immunity

Immunity for covered financial institutions

A covered financial institution shall not be liable, including in any civil or administrative proceeding, for a disclosure made by an individual described above if the individual was employed by the covered financial institution at the time of the disclosure; and
(before the time of the disclosure), each individual described received the training described.

Question Three

Where and how do we report suspected elder financial abuse?

- A. The local police.**
- B. It may depend on the specific concerns, use your resources to identify the correct agency.**
- C. Any known family member, even if they are not joint on the account.**
- D. It's not really your problem, no need to get involved.**

Reporting

PENNSYLVANIA NEIGHBORHOOD MAP

State: Neighborhood | [List](#)

ADULT PROTECTIVE SERVICES
Pennsylvania Adult Protective Services
Hotline: 1-800-490-8505

THE NEIGHBORHOOD OF RESOURCES INVOLVED IN AN ELDER ABUSE CASE

<https://www.justice.gov/elderjustice/support/resources-neighborhood>


Adult Protective Services (APS)

A state social service program that can take reports of alleged abuse, or neglect/self-neglect of vulnerable adults age 18 or older. APS can assess and determine the needs of the elder abuse victim. Some professionals are mandatory reporters.

Reporting

Home » Elder Justice Initiative (EJI) » Financial Exploitation SHARE en Español

ELDER ABUSE RESOURCE ROADMAP - FINANCIAL



Who caused you (or someone you know) financial loss?

Select one option

Someone You Know and Trust

A Financial Professional

A Stranger or Unknown Person

Someone Connected to Your Nursing Home

[View All Financial Exploitation Topics](#)

<https://www.justice.gov/elderjustice/roadmap>

Reporting

SOMEONE CONNECTED TO NURSING HOME

What happened at the Nursing Home?

Select one option

Nursing Home Billing Fraud

VA Extended Care or VA Home Care Fraud

Lost or Stolen Government Benefits

Theft, Neglect, Physical and Sexual Abuse

Home » Elder Justice Initiative (EJI)

SHARE

en Español

SOCIAL SECURITY FRAUD, MISUSE, OR IMPERSONATION

Social Security Fraud & Misuse

The Social Security Administration (SSA) investigates reports like these:

- Providing false information or evidence for a benefit claim
- Concealment of work and assets
- Representative payee misuse
- Misuse and trafficking of Social Security numbers and cards by people or businesses
- Reports of criminal activity and serious misconduct involving Social Security employees

File a Report with SSA

Or call **1-800-269-0271**.

What Happens Next?

- SSA's Office of Inspector General (OIG) reviews all reports that are filed.
- SSA OIG cannot provide you with information about actions taken on any reports.

Exploitation by a Caregiver

Russell, 88, needed help managing his day-to-day affairs. His nephew, Jack was out of work and offered to come and live with Russell and help him while Jack looked for a job. Jack took his uncle to the bank saying he wanted to protect Russell's money. Russell told the bank teller to add Jack to his bank accounts. Jack then downloaded a power of attorney (POA) form from the Internet and had Russell sign it. With the POA, Russell's credit card company added Jack as a second user to his credit card. When Russell's sister visited him, she asked about the situation. Russell told her that he thought their nephew was stealing his money. She and Russell went to the bank and learned that Jack had spent a considerable amount of his uncle's money. The sister alerted bank officials, Adult Protective Services (APS) and local law enforcement. Russell filed for an emergency civil protective order to have Jack removed from his home.

What Should You Do?



Provide members with financial literacy education and reporting guidance.

Train staff to detect and report elder financial exploitation.

Use the NCUA and other federal resources and guidance to improve credit union programs and policies.

Resources

www.olderadultnestegg.com – Peter Lichtenberg @ Wayne State, Institute of Gerontology

AARP elder financial resources – www.aarp.org/banksafe

<https://www.medicareadvantage.com/complete-guide-to-elder-financial-abuse>

NCUA Scams Targeting Seniors & Reporting Elder Financial Abuse Videos on YouTube

NCUA Letter to Credit Unions 13-CU-08 and accompanying interagency guidance

<https://www.ncua.gov/files/letters-credit-unions/ElderAbuseGuidance.pdf>

Resources

Immunity from suit for disclosure of financial exploitation of senior citizens:

<https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title12-section3423&num=0&edition=prelim>

<https://www.justice.gov/elderjustice/support/resources-neighborhood>

<https://www.justice.gov/elderjustice/roadmap>

<https://www.justice.gov/elderjustice/prosecutors/statutes>

FBI's Internet Crime Complaint Center - www.IC3.gov

Phone Resources

For non-life-threatening emergencies, the Department of Justice recommends you call either:

National Elder Fraud Hotline

1-833-FRAUD-11 (or 833-372-8311)

6AM - 11PM Eastern Time

Eldercare Locator helpline

1-800-677-1116



Cindy Hagan

Compliance and Fraud
Risk Director

chagan@vfccu.org

