ELDER FINANCIAL EXPLOITATION

How to Protect Your Customers

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

ABA FOUNDATION®

ELDER FINANCIAL EXPLOITATION

What is Elder Financial Exploitation?

Elder financial exploitation (EFE) is the illegal or improper use of an older person's funds, property, or assets. It is the fastest-growing form of elder abuse, as perpetrators may be family members, friends, neighbors, caregivers, health care providers, business associates, or strangers.

EFE crimes generally fall into two categories:

ELDER THEFT

Trusted individuals steal money or belongings from seniors. Elder theft comprises two-thirds of EFE cases. Examples:

- Forging checks
- Stealing retirement or Social Security benefits
- Using credit cards or bank accounts without permission
- Changing names on wills, bank accounts, life insurance policies, or real estate titles without permission

ELDER SCAMS

Strangers deceive older adults into transferring money to them for promised goods, services or financial benefits which do not exist or were misrepresented. Examples:

- **Tech support scams** — Scammers pose as tech repair agents to access victims' computers and finances
- **Investment scams** — Perpetrators induce investors to make purchases based on false information and promises of large returns with minimal risk
- **Romance scams** — Criminals seek money from victims on dating apps and social media
- **Government or family imposter scams** — Fraudsters impersonate government officials or family members to demand money
- **Lottery scams** — Criminals claim victims must pay taxes or fees to access winnings from a lottery or raffle

The Impact on Seniors and the Economy

The average loss per older adult was **$35,101** in 2022, according to the FBI Internet Crime Complaint Center. The FBI reported total losses increased **84%** between 2021 and 2022.

Victims may lose their life's savings or their homes. Victims may also experience fear, shame, anxiety, and depression. Some may lose their independence or even their lives.

EFE costs seniors billions of dollars annually. It also hurts businesses, families, and government programs. EFE may force older adults to become reliant on government-sponsored assistance programs.

Why Older Adults Are Targeted

Seniors generally have more accumulated wealth, thanks to a lifetime of working, investing, and saving. Older adults who are most vulnerable to exploitation may:

- Have previously been a victim of fraud or scams
- Suffer from mild cognitive impairment or dementia
- Be dependent on others to meet daily needs
- Experience social isolation
- Lack information about scams and fraud
- Be unfamiliar with technology, online services, and safe online behavior

It is important to note that any age demographic can be victimized, not just older adults.

For More Information, Visit:

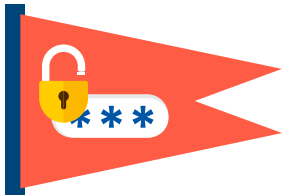
- ABA Foundation's Older Americans Resource Page — aba.com/olderamericans
- Federal Bureau of Investigation — fbi.gov
- Department of Justice — justice.gov/elderjustice/financial-exploitation
- Internet Crime Complaint Center — ic3.gov
- Consumer Financial Protection Bureau — consumerfinance.gov
- Federal Trade Commission — ftc.gov
- National Center on Elder Abuse — ncea.acl.gov
- National Adult Protective Services Association — napsa-now.org

SPOT THE RED FLAGS OF ELDER FINANCIAL EXPLOITATION

ABA FOUNDATION®

SPOT THE RED FLAGS OF ELDER FINANCIAL EXPLOITATION

Recognize the signs of elder financial exploitation, such as changes in behavior or unusual account activity.



Watch for customers who:

- Make sudden and unusual changes to their accounts, such as altering contact information or adding new contacts who are located overseas
- Cannot explain unusual account activity or appear confused about financial transactions
- Appear distressed, fearful, and anxious to follow directions provided by others (e.g., they're receiving instructions while on their cellphone)
- Seem fearful of, or submissive to, a caregiver
- Indicate a transaction is for, or on behalf of, an online friend or romantic partner
- Urgently want to send money to a loved one because of an emergency, but the recipient is an unconnected individual or third-party business
- Indicate an interest in purchasing large numbers of gift cards or prepaid access cards
- Send multiple checks or wire transfers with memos such as "tech support services," "winnings," "taxes," "home improvement," "investment," or "crypto investment"
- Close CDs or accounts without regard for penalties
- Suddenly discuss buying cryptocurrency

Be wary of accompanying individuals who:

- Are excessively interested in the customer's finances
- Do not allow the older customer to speak
- Are conducting financial transactions on the customer's behalf without proper documentation or with possibly forged documents

Look out for accounts with:

- Uncharacteristic, sudden, abnormally frequent, or significant cash withdrawals or funds transfers
- Repeated daily maximum currency withdrawals from ATMs
- Uncharacteristic attempts to wire large sums of money
- Debit transactions which are inconsistent with established patterns
- Sudden or frequent non-sufficient fund activity
- Statements mailed to locations other than the customer's home

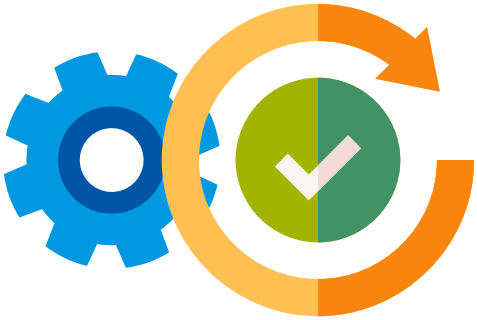
Source: FinCEN Advisory on Elder Financial Exploitation, FIN-2022-A002

ABA FOUNDATION

COMBAT ELDER FINANCIAL EXPLOITATION WITH THE THREE Rs:

RECOGNIZE

RESPOND



REPORT

ABA FOUNDATION®

COMBAT ELDER FINANCIAL EXPLOITATION WITH THE THREE Rs: RECOGNIZE, RESPOND, REPORT

Help protect your older adult customers by following the 3-R framework:

Recognize

- Learn the financial and behavioral red flags of elder financial exploitation (EFE)
- Question the suspicious transaction or activity. Don't be afraid to ask:
  - ✦ The purpose of the funds transfer, cashier's check, or wire
  - ✦ How the customer knows the individual(s) receiving the funds
  - ✦ If the customer was coached by someone on how to answer the bank's questions
- Review the prior history of the account. Watch for recent changes or uncharacteristic behavior such as:
  - ✦ Frequent deposits, quickly followed by funds transfers to multiple external accounts
  - ✦ The addition of a new signer, contact, or Power of Attorney
  - ✦ A new companion accompanying the customer to transfer funds
  - ✦ Sudden and large cash withdrawals
  - ✦ Unusual domestic or international wires/funds transfers

Respond

- Contact the customer's trusted third-party contact, if available
  - ✦ Further scrutiny of the account may be needed if the trusted third party was recently added
- Escalate the transaction to the appropriate level of management
- Delay or refuse a transaction, as allowed under state law and bank policy

Report

- Report suspicious activity according to your bank's protocols
  - ✦ Follow internal procedures for reporting suspicious activity, which may trigger a Suspicious Activity Report
  - ✦ The bank may be required to report suspected abuse to Adult Protective Services and/or law enforcement
- Strongly encourage fraud and scam victims to file a complaint with the Internet Crime Complaint Center at IC3.gov, or offer to file on their behalf

ABA FOUNDATION