Spotting Red Flags of Elder Financial Exploitation in your Institution

October 27, 2016

ACAMS Greater Philadelphia Chapter

AGENDA

- Evolution of Elder Abuse/Financial Exploitation
- Recommendations
- Red Flags
- Case Scenarios
- Preventive Measures
- Identity Theft Recovery Steps
- Stetson Law
- Q&A
- Contact & Reference Information

Elder Abuse

Elder abuse has steadily been on the rise across the world.

Elder financial exploitation has been called the crime of the 21st century and deploying effective interventions has never been more important. Older people are attractive targets because they often have assets and regular income. These consumers may be especially vulnerable due to isolation, cognitive decline, physical disability, health problems, or bereavement. Elder financial exploitation robs victims of their resources, dignity and quality of life; and they may never recover from it.

Financial institutions play a vital role in preventing and responding to this type of elder abuse. Banks and credit unions are uniquely positioned to detect that an elder account holder has been targeted or victimized, and to take action.

FinCEN Advisory

On February 22, 2011, the Financial Crimes Enforcement Network (FinCEN) issued an advisory to assist the financial industry in reporting instances of financial exploitation of the elderly, a form of elder abuse.

Financial institutions can alert appropriate authorities to suspected elder financial exploitation. FinCEN has notified the public about this upward trend, using SARs as an important method to identify this form of financial exploitation.

There are important RED FLAGS relating to financial exploitation of the elderly.

<u>FinCEN's Advisory states:</u>

- In the instances where elderly individuals experience declining cognitive or physical abilities, they may find themselves more reliant on specific individuals for their physical well-being, financial management, and social interaction.

- Although anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

Recommendations

Per Consumer Financial Protection Bureau:

- **Train management and staff to prevent, detect and respond**. Train personnel regularly and frequently, and tailor training to specific staff roles. Training should cover warning signs that may signal financial exploitation, including behavior and transactions that are red flags, and action steps to prevent exploitation and respond to suspicious events.
- **Use technology to monitor for signs of elder financial exploitation**. Because indicators of elder fraud risk may differ from conventionally accepted patterns of suspicious activity, financial institutions using predictive analytics should review their filtering criteria against individual account holders' patterns and explore additional risk factors that may be associated with elder financial exploitation.
- **Report all cases of suspected exploitation to relevant federal, state and local authorities**. Make timely reports whenever financial institutions spot activity that signals financial exploitation, regardless of whether reporting is mandatory or voluntary under state or federal law. Reporting does not, in general, violate the privacy provisions of the Gramm-Leach-Bliley Act.

Recommendations

- **File Suspicious Activity Reports (SARs).** The Financial Crimes Enforcement Network (FinCEN) issued an Advisory in 2011 noting that SARs are a valuable reporting avenue for these cases. FinCEN now designates "elder financial exploitation" as a category of suspicious activity and provides a checkbox for it on the electronic SAR form. File SARs for elder financial exploitation when mandatory under the Bank Secrecy Act and consider filing them voluntarily in other cases.
- **Expedite documentation requests from Adult Protective Services (APS), law enforcement and other government entities investigating reports of financial exploitation.** Provide documents at no charge.
- **Comply with the Electronic Fund Transfer Act (EFTA) and Regulation E.** Per Regulation E, extend time limits for consumer notification of an unauthorized transaction under extenuating circumstances such as hospitalization. Do not impose greater consumer liability than Regulation E allows, even when an older consumer may appear to be negligent by, e.g., noting a PIN on or near a debit card.

Recommendations

- **Enable older account holders to consent to information sharing with trusted third parties**. Establish procedures so consumers can provide advance consent to sharing account information with a designated trusted third party when the financial institution reasonably believes that the consumer may be at risk of financial abuse.
- **Offer age-friendly services that can enhance protections against financial exploitation**. Provide consumers with information about planning for incapacity. Honor powers of attorney unless there is a basis in state law to refuse them. Offer opt-in account features such as cash withdrawal limits, geographic transaction limits, alerts for specified account activity, and view-only access for authorized third parties. Where appropriate, offer multi-party accounts without right of survivorship (convenience accounts or agency accounts) as good alternatives to traditional joint bank accounts.
- **Work with law enforcement and Adult Protective Services. Develop relationships with law enforcement and APS personnel to facilitate timely response to reports**. Provide expert consultation and document review to assist with case investigations, including through multidisciplinary teams engaging in case review.
- **Coordinate efforts to educate older account holders, caregivers and the public**. Work with an array of agencies and service organizations to offer educational programs and distribute materials. Participate in multidisciplinary network initiatives.

Red Flags

- ✓ **Suspicious changes in wills or powers of attorney** – Out of the blue, your grandfather wills all of his belongings to his new nurse.
- ✓ **Financial activity the person couldn't have done herself** – You discover repeated ATM withdrawals from your bedridden mother's bank account.
- ✓ **Bills not being paid** – When visiting a neighbor, you see mail piling up on his desk. Maybe his caregiver is using his money for something other than paying bills.
- ✓ **Significant withdrawals or unusual purchases** – You notice charges for fancy electronics on your thrifty aunt's credit card bill.

Red Flags

Transaction pattern changes:

- ✓ Abrupt increases in withdrawals; new spending patterns following the addition of a new authorized user; atypical ATM withdrawals; unusual gaps in check numbers.

Identity theft and coercion:

- ✓ Address changes followed by account changes; new third party speaking for the older adult; older consumer is confused by or unaware of account changes; requests to send account statements to a third party's address.

Behavioral changes:

- ✓ Older consumer appears newly distressed, unkempt, or unhygienic; older consumer mentions lottery or sweepstakes opportunities or winnings; older adult inquires about international wire transfers.

Using vignettes or case studies to illustrate plausible scenarios may enable staff to understand and remember the red flags.

Case Scenarios

The following are a few case examples from news reports to illustrate the ways that a variety of perpetrators exploit older consumers. In all of these cases, funds went from the victims' deposit accounts to the perpetrators.

- A Minnesota pastor persuaded a man suffering from Alzheimer's and Parkinson's diseases to allow him to manage his finances. The pastor made over 130 withdrawals from the older man's bank account and was later convicted of stealing about $25,000.
- Prosecutors charged an Indiana home care worker with nine felonies after she took more than $150,000 from a 79-year-old woman with dementia. The caregiver stole the funds through transactions on multiple credit cards, checks drawn on a savings account and cashed certificates of deposit. A bank fraud analyst was the first to detect the unusually large credit card charges, and the analyst called Indiana Adult Protective Services.
- An Oklahoma woman received mail and phone calls telling her that she had won a sweepstakes and would get prizes if she sent money to collect her winnings. She sent as many as 90 checks a month, in response to requests for payments of $50 to $2,000. A bank employee discovered the losses when the victim asked how she could send a large amount of cash through the mail.

Preventive Measures

Asking customers to explain and confirm transactions that raise red flags, e.g.:

- With a large cash withdrawal ("This is an unusually large withdrawal, are you sure you want cash?")
- With wire transfers, ("Have you taken steps to be sure the recipient is trustworthy?")
- With large online transactions ("I'm calling to confirm your recent online banking activity because the transfer is a large amount.")
- When a third party accompanies the account holder and other red flags are present ("Can we talk privately for a moment?")

Instructions for recognizing signs of diminished capacity with action steps for frontline staff to follow when signs are observed in customers

- Examples such as memory loss, communication problems, calculation problems and disorientation may be signs of diminished capacity in a customer
- Educating older customers on common scams and fraud ("Have you read up on the latest telemarketing scams? Here's a flyer to take home and to share with friends and family.")

Preventive Measures

Instructions for recognizing signs of diminished capacity with action steps for frontline staff to follow when signs are observed in customers:

- Examples such as memory loss, communication problems, calculation problems and disorientation may be signs of diminished capacity in a customer
- Educating older customers on common scams and fraud ("Have you read up on the latest telemarketing scams? Here's a flyer to take home and to share with friends and family.")

Identity Theft Recovery Steps

What to do right away - Are you dealing with tax, medical, or child identity theft? (Special forms for specific situations)

- **Step 1: Call the companies where you know fraud occurred.**
- **Step 2: Place a fraud alert and get your credit reports.**
- **Step 3: Report identity theft to the FTC.**

You may choose to file a report with your local police department.

<u>What to do Next – Repair the damage</u>

- **Close new accounts opened in your name.**
- **Remove bogus charges from your accounts.**
- **Correct your credit report.**
- **Consider adding an extended fraud alert or credit freeze.**

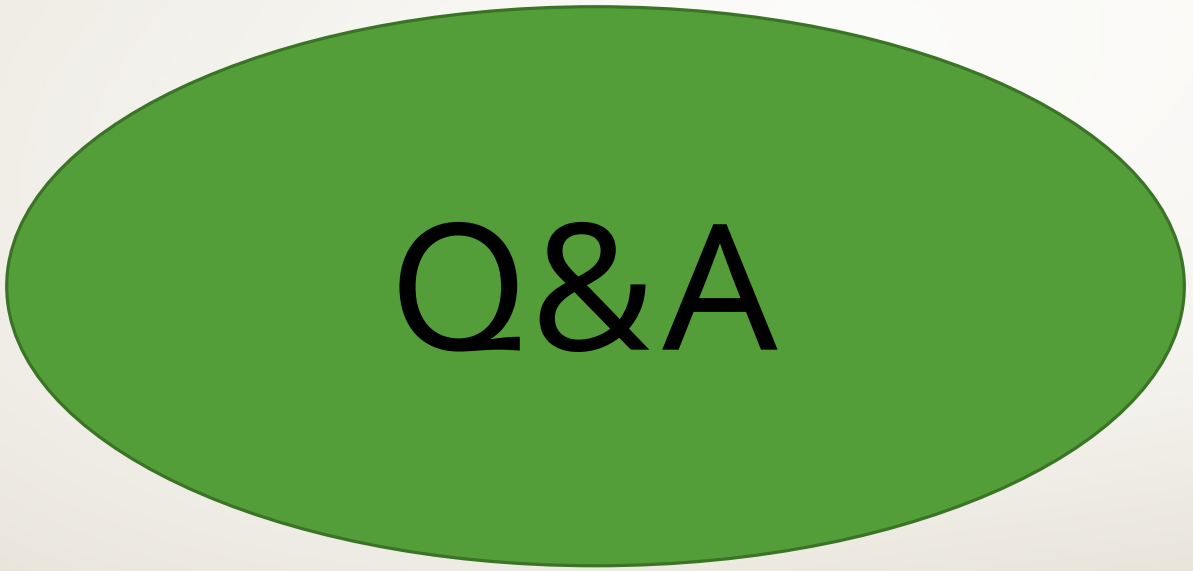
<u>Other Possible Steps</u>

- **Report a misused Social Security number.**
- **Stop debt collectors from trying to collect debts you don't owe.**
- **Replace government-issued IDs.**
- **Clear your name of criminal charges.**

Stetson Law

All states (not territories) have a mandatory reporting statute for elder abuse, however, almost every state varies as to the following areas:

- **Who is required to report abuse or suspected abuse (the "mandated reporters").**
- **What activities constitute or require reporting**
- **Whether or not the victim lacks capacity**
- **Whether or not the victim resides at home or in an assisted living facility or nursing home.**


Q&A

Reference Information

Financial Crimes Enforcement Network (FINCEN)

https://www.fincen.gov/

Consumer Finance Protection Bureau (CFPB)

http://www.consumerfinance.gov/

Mandatory Reporting by U.S. States and Territories (as of March 2016)

http://www.stetson.edu/law/academics/elder/ecpp/media/Mandatory%20Reporting%20Statutes%20for%20Elder%20Abuse%202016.pdf