

BITS Fraud Protection Toolkit

Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation

April 2010

© BITS 2010.



Agenda

- **Background**
- **Financial Exploitation Defined**
- **Role of Financial Institutions**
- **Red Flags, Offenders and Scams**
- **How to Make a Difference**
 - **Role of the Customer Contact Staff**
 - **Role of the Loss Prevention Department**
 - **Role of Adult Protective Services (APS)**
- **Resources for Financial Institutions and Consumers**



Vulnerable Adult Abuse: Background

■ Vulnerable Adults

- Defined as over the age of 60 – 65, depending on the state, or disabled individuals over the age of 18.
- Often lack the physical and mental capability of caring for themselves.

■ Often traced to family members, caregivers and trusted friends.

■ Adult Protective Services (APS) agencies substantiate more cases of financial abuse than physical abuse each year.



Vulnerable Adult Abuse: Statistics

- A 2008 survey by the University of Chicago reports approximately 13 percent of elderly Americans have been verbally mistreated (9%) or financially exploited (3.5%) or taken advantage of.
- In a telephone survey of more than 5,500 older adults, 5.2% of respondents reported current financial exploitation by a family member and 6.5% reported lifetime financial exploitation by a non-family individual.
- Only 1 of 14 cases of domestic vulnerable adult abuse incidences is reported.
 - Number of cases exceeds 850,000 annually
- By 2030, the number of Americans aged 65 and older will more than double to 71 million, making up roughly 20 percent of the U.S. population.



Vulnerable Adult Abuse: Financial Exploitation

- **Financial exploitation can include:**
 - **Illegal or improper use of a vulnerable adult’s funds, property or assets.**
 - **Cashing checks without authorization or permission.**
 - **Forging an older person’s signature.**
 - **Misusing or stealing an older person’s money or possessions.**
 - **Coercing or deceiving an older person into signing any document.**
 - **Contracts**
 - **Wills**
 - **Improper use of conservatorship, guardianship, or Power of Attorney.**



Vulnerable Adult Abuse: Role of the Financial Institution

- A primary role of financial institutions is to protect assets, prevent losses and safeguard consumer information.
- Regular customer contact puts financial institutions in a unique position to detect behavior changes and to assist in protecting customers.
- Proactive measures help to promote goodwill within the communities where institutions have footprints.
- Currently, 20 states and the District of Columbia require financial institutions to report suspected cases of financial abuse of the elderly



Financial Exploitation Categories

■ Theft of Income:

- Most common form of financial exploitation.
- Typically less than \$1000 per transaction.

■ Theft of Assets

- Often more extensive and typically involves abuse associated with:
 - Power of Attorney
 - Real estate transaction
 - Identity theft
 - Tax manipulation



Types of Scams

- **Advance fee fraud or “419” frauds**
 - See appendix for a list of variations of these schemes
- **Debt relief scams**
- **Exploitation by a financial institution employee**
- **Fictitious relative**
- **Financial institution examiner impersonation fraud**
- **Foreclosure rescue scam**
- **Identity theft**



Types of Scams, continued

- Misappropriation of income or assets
- Pigeon drop
- Power of Attorney fraud
- Reverse mortgage scam
- Sweetheart scam
- Telemarketing or charity scams
- Unsolicited work



Vulnerable Adult Abuse: Relative and Caregiver Offenders

- Have a unique position of trust and ongoing relationship with the vulnerable adult.
- Perpetrators take advantage of the victim and rationalize their actions in various ways. e.g., Perpetrators may feel that they are entitled to receiving their inheritance early and do not view their actions as wrong.



Vulnerable Adult Abuse: Relative and Caregiver Offenders

- **Methods of financial exploitation by relatives and caregivers include:**
 - Theft of the victim's money or other cash-equivalent assets.
 - Borrowing money with no intent to repay.
 - Cashing or keeping some portion of the person's pension, Social Security or other income checks without permission.
 - Using the victim's checks or ATM, debit or credit cards without permission.
 - Transferring title on, or re-encumbering, real property of the vulnerable adult.
 - Opening or adding their name to banking accounts without the elder's permission.

“Red flags” that could indicate actual or potential fraud

Changes to Accounts and/or Documentation

- Recent changes or additions of authorized signers on a vulnerable adult’s financial institution signature card.
- Statements are sent to an address other than the vulnerable adult’s home.
- Vulnerable adult has no knowledge of a newly-issued ATM, debit or credit card.
- Abrupt changes to, or confusion regarding changes in, financial documents such as Power of Attorney, account beneficiaries, wills and trusts, property titles, deeds and other ownership documents.

“Red flags” that could indicate actual or potential fraud

Changes to Accounts and/or Documentation

- Sudden unexplained transfers of assets, particularly real property.
- Sudden appearance of previously uninvolved relatives claiming their rights to a vulnerable adult’s affairs and possessions.
- Discovery of a vulnerable adult’s signature being forged for financial transactions or for the titles of his or her possessions.
- Refinance of the vulnerable adult’s property, particularly with significant cash out or with the addition of new owners on the deed and, most particularly, without the new owners shown as co-borrowers on the loan.

“Red flags” that could indicate actual or potential fraud

Changes in Spending and Transaction Patterns

■ Checks

- A set of “out-of-sync” check numbers.
- A sudden flurry of “bounced” checks and overdraft fees.
- Transaction review shows multiple small dollar checks posting to the senior’s account in the same month. This could be indicative of telemarketing or charity scams.
- Large withdrawals from a previously inactive account or a new joint account.
- Account use shortly after the addition of a new authorized signer.

“Red flags” that could indicate actual or potential fraud

Changes in Spending and Transaction Patterns

■ Credit/Debit

- Large withdrawals from a previously inactive account or a new joint account.
- Abrupt increases in credit or debit card activity.
- Sudden appearance of credit card balances or ATM/debit card purchases or withdrawals with no prior history of such previous use.

“Red flags” that could indicate actual or potential fraud

Changes in Spending and Transaction Patterns

■ Credit/Debit, continued

- Withdrawals or purchases using ATM or debit cards that are:
 - Repetitive over a short period of time;
 - Inconsistent with prior usage patterns or at times (e.g., late night or very early morning withdrawals by elderly customers, withdrawals at ATMs in distant parts of town by customers who don't drive or are house bound.); or
 - Used shortly after the addition of a new authorized signer.

“Red flags” that could indicate actual or potential fraud

- Unexplained disappearance of funds or valuable possessions, such as safety deposit box items.
- Vulnerable adult appears confused about the account balance or transactions on his or her account.
- A caregiver appears to be getting paid too much or too often.
- Significant increases in monthly expenses paid which may indicate that expenses for persons other than the customers are being paid.
- Sudden changes in accounts or practices, such as unexplained withdrawals of large sums of money, particularly with a vulnerable adult who is escorted by another (e.g., caregiver, family member, “friend”) who appears to be directing the changing activity patterns.

“Red flags” that could indicate actual or potential fraud

Changes in Appearance or Demeanor

- Vulnerable adult has a companion who seems to be “calling the shots”.
- Change in the vulnerable adult’s physical or mental appearance. For example, the customer may appear uncharacteristically disheveled, confused or forgetful. These signs could indicate self neglect or early dementia and leave the vulnerable adult open for financial exploitation.

“Red flags” that could indicate actual or potential fraud

Changes in Appearance or Demeanor

- Vulnerable adult acknowledges providing personal and account information to a solicitor via the phone or email.
- Excitement about winning a sweepstakes or lottery.
- Allegations from a vulnerable adult or relative regarding missing funds or physical or mental abuse.

Internal Awareness and Training: Role of the Customer Contact Staff

- **If you suspect fraud:**
 - **Carefully verify the transactional authority of person(s) acting on the customer's behalf.**
 - **Avoid confrontation and attempt to separate the vulnerable adult from the individual accompanying him or her.**

Internal Awareness and Training: Role of the Customer Contact Staff

■ If you suspect fraud:

- Use probing questions to determine the customer’s intent. It is important to let the customer express their intent using his or her own words without prompting. For example:

- *Power of Attorney (POA) request:* “Mr. Jones, do you want Ms. Smith to be able to withdraw money from your account at any time without needing your permission?”
- *Home repair or 419 scam:* “Mrs. Green, \$4000 is a lot of cash to be carrying around. For your safety, I can make a check out to the other party if you have the receipt with the correct spelling of the name.”

Internal Awareness and Training: Role of the Customer Contact Staff

■ If you suspect fraud:

- Share an “awareness” document with information about common schemes with consumers to read prior to receipt of large out-of-pattern withdrawals.
- Delay the suspicious transaction, if possible, by advising the customer that additional verification of the transaction is required.
- Contact loss prevention and/or legal departments for assistance and guidance.

Internal Awareness and Training: Role of the Loss Prevention Dept.

- Document the situation.
- Take immediate protective action on accounts by placing holds or restraints and follow normal prevention and recovery steps to follow the money as needed.
- Report the incident to law enforcement following your institution's normal protocol.
- Make a verbal report to the local APS and provide investigative research and services. Continue to monitor the account during legal proceedings, if necessary.
- Advise customer contact staff and appropriately document files of final outcome.

Internal Awareness and Training: Role of Adult Protective Services

- Receive and investigate reports.
- Make unannounced visit to vulnerable adult's home.
- Offer services when abuse is confirmed.
- Work with legal service providers and law enforcement to prosecute those responsible for abuse.
- Advise financial institution of outcome as it relates to the institution's accounts.

Internal Awareness and Training: Role of Legal Departments

- **Certain protections exist for financial institutions when reporting suspicious activity**
 - **The Right to Financial Privacy Act of 1978 applies only to federal agencies requesting consumer information from financial institutions.**
 - **Gramm-Leach-Bliley Act applies to federal, state and local agencies, but it contains several exemptions that permit disclosure, including “to protect against or prevent actual or potential fraud, unauthorized transaction, claims, or other liability”.**
 - **49 states and the District of Columbia include immunity provisions in their APS laws that protect individuals who make reports in good faith. These immunity provisions may be interpreted as overriding the restrictions in applicable state privacy law.**

Internal Awareness and Training: Role of Legal Departments

- Financial institutions should consult with legal departments on the specific reporting guidelines for the states in which they do business.
- For more information see:
 - *Can Bank Tellers Tell? Reporting Financial Abuse of the Elderly* (American Bar Association)
 - *Legal Issues Related to Bank Reporting of Suspected Elder Financial Abuse* (American Bar Association)
 - National Center on Elder Abuse (NCEA), <http://www.ncea.aoa.gov>
 - List of state-specific laws, data and statistics, and statewide resources.
 - Adult Protective Services, Institutional Abuse and Long Term Care Ombudsman Program Laws: Citations, by state.

Resources

■ Agencies and Associations

- Department of Health and Human Services, Administration on Aging (AoA), <http://www.aoa.gov>
- National Adult Protective Services Association (NAPSA), <http://apsnetwork.org>
- National Center on Elder Abuse (NCEA), <http://www.ncea.aoa.gov>
- National Center for Victims of Crime, <http://www.ncvc.org>
- National Organization of Triads, Inc. (NATI) <http://www.nationaltriad.org>

Resources

Training Materials and Toolkits

- Attorney General of Texas – Senior Texans Page, <http://www.oag.state.tx.us/elder/index.shtml>
- Clearinghouse on Abuse and Neglect of the Elderly (CANE), <http://www.cane.udel.edu>
- California Banker's Website, <http://www.calbankers.com>
- Elder Financial Protection Network (EFPN), <http://bewiseonline.org>
- Elder Abuse Training Program, <http://www.medifecta.com/>
- Federal Bureau of Investigation (FBI)
 - Fraud poster, http://www.fbi.gov/majcases/fraud/fraud_alert.pdf
 - Fraud schemes, <http://www.fbi.gov/majcases/fraud/fraudschemes.htm> or <http://www.fbi.gov/majcases/fraud/seniorsfam.htm>

Resources

Training Materials and Toolkits, continued

- **Fiduciary Abuse Specialist Team (FAST),**
<http://www.preventelderabuse.org/communities/fast.html>
- **Financial Institution Elder Abuse Training Kit,**
<http://www.oregonbankers.com/community/efapp>
- **The Massachusetts Bank Reporting Project: An Edge Against Elder Financial Exploitation, contact Jonathan Fielding,**
jonathan.fielding@state.ma.us
- **Missouri Department of Health and Human Services – Missourians Stopping Adult Financial Exploitation (MOSAFE) Project,** <http://www.dhss.mo.gov/MOSAFE/index.html>
- **Stetson University Consumer Protection Education Project,**
<http://www.law.stetson.edu/elderconsumers>

Resources

■ Consumer Resources

- AARP Foundation and Colorado Attorney General's ElderWatch Project, <http://www.aarpelderwatch.org/>
- Attorney General of Texas – Senior Texans Page, <http://www.oag.state.tx.us/elder/index.shtml>
- Federal Bureau of Investigation (FBI)
 - Common fraud schemes, <http://www.fbi.gov/majcases/fraud/fraudschemes.htm>
 - Frauds targeting senior citizens, <http://www.fbi.gov/majcases/fraud/seniorsfam.htm>
- Federal Deposit Insurance Corporation (FDIC) <http://www.fdic.gov/consumers/consumer/news/cnfall05/index.html>
- Federal Trade Commission (FTC), <http://www.ftc.gov/bcp/index.shtml>
 - FTC identity theft assistance center, <http://www.ftc.gov/idtheft>

Resources

■ Consumer Resources, continued

- MetLife Mature Market Institute® (MMI),
www.maturemarketinstitute.com

- Tip sheet,

- <http://www.metlife.com/assets/cao/mmi/publications/consumer/mmi-helpful-hints-preventing-elder-financial-abuse-olderadults.pdf>

- Guides,

- <http://www.metlife.com/mmi/publications/since-you-care-guides/index.html>

- North American Securities Administrators Association, Inc (NASAA),
http://www.nasaa.org/Investor_Education/NASAA_Fraud_Center

For More Information

Heather Wyson

Director, BITS Fraud Program

202.589.4322

heather@fsround.org

Paper: www.BITS.org/Publications/Fraud

Appendix

- **Variations of Advance Fee and “419” Frauds**
 - Charitable donation scam
 - Fake prizes
 - Government grant scams
 - Home Stealing
 - Inheritance scams
 - International lottery and sweepstakes fraud
 - Internet sales or online auction fraud
 - Investment Property
 - Pharming
 - Recovery Room Scams
 - Spoofing
 - Work-from-Home Scams