THE FINANCIAL SERVICES ROUNDTABLE

Financing America's Economy

BITS

FINANCIAL SERVICES ROUNDTABLE

At-Risk Adult Training Curriculum

February 2013

The Financial Services Roundtable and BITS
1001 Pennsylvania Avenue NW
Suite 500 South
Washington, DC 20004
(202) 289-4322

At-Risk Adult Training Curriculum

The following document provides an outline for institutions to leverage in developing internal training programs on financial abuse of at-risk adults. This document is intended to complement the BITS publication *Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation*[1].

This curriculum provides a general overview for institutions designing their internal training programs. Institutions should consult state and local legal requirements to ensure their institution's training is compliant.

This document covers the following:

Developing an Internal Training Seminar

This section outlines suggestions regarding the content and frequency of a training program for financial institution front-line, customer-facing personnel.

Additional Training for Fraud Investigators

This section provides further suggestions for additional training content for financial institution employees working in fraud investigation. These employees deal with the outcomes of fraudulent activity against vulnerable individuals and, therefore, should have additional knowledge.

Three appendices provide key messaging content for communications material directed to these constituencies:

Appendix A: For Senior Customers
Appendix B: For Family Members and Fiduciary
Appendix C: For Financial Institution Staff

For more information about this or other BITS/Roundtable publications, contact bits@fsround.org.

About The Financial Services Roundtable/BITS

The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America's economic engine, accounting directly for $98.4 trillion in managed assets, $1.1 trillion in revenue, and 2.4 million jobs. BITS, the technology policy division of the Roundtable addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services.

[1] Available at http://www.bits.org/publications/fraud/BITSProtectingVulnerableAdults0410.pdf.

Developing an Internal Training Seminar

Frequency. All new employees should receive an initial training. Employees in consumer-facing and high-risk roles (financial institutions[2] and banking and call centers) should receive a thorough annual training. In an effort to minimize the employee's time, this training can be incorporated into compliance or loss prevention training and may complement the institutions anti-money laundering (AML) compliance program. Depending on accessibility of employees, the training can be offered as a web-based training followed by a knowledge assessment.

To reinforce the messages institutions may provide regular (e.g., quarterly) communications. These may include one page tip documents. The appendices provide sample tips, which institutions may use in communicating to their employees and consumers.

Content

1.0 Background

1.1 Definitions

1.1.1 **Adult Protective Services (APS)** – An organization established by individual state statutes that investigates reports alleging abuse, neglect and exploitation of elderly and disabled adults, and intervenes to protect vulnerable adults who are at risk.

1.1.2 **Area Agency on Aging (AAA)** – A nationwide network of state and local programs that help older people plan and care for their life-long needs. Services include information and referral for in-home services, counseling, legal services, adult day care, skilled nursing care/therapy, transportation, personal care, respite care, nutrition and meals.

1.1.3 **At-Risk Adult** – A person who is either being or in danger of being mistreated and/or exploited, and who due to age and/or disability, is unable to protect him/herself. At-risk adult is also a commonly used term. State and federal requirements may refer to an at-risk adult as a vulnerable adult or elder.

1.1.4 **Diminished mental capacity** – Permanent or gradual impairment of an individual's cognitive abilities, which may limit their capacity to make sound decisions regarding their investments and finances. This impairment may not be apparent in at-risk adults. Recent medical studies suggest mental impairment regarding financial matters may occur before general cognitive impairment is obvious.

1.1.5 **Fact Pattern** – Legal phrase referring to the summary of what took place in a case for which relief is sought.

[2] An establishment that focuses on dealing with financial transactions, such as investments, loans and deposits (e.g., banks, trust companies, insurance companies and investment dealers).

1.1.6 **Fiduciary** – An individual appointed (1) guardian by a court of another person's property or (2) to act on behalf of another person, by that person in a legal document known as a Power of Attorney. Unlike people in ordinary business relationships, fiduciaries may not seek personal benefit from their transactions with those they represent. In addition, an individual may appoint a lay fiduciary, which is often a family member or close friend with limited financial knowledge.

1.1.7 **Elder (At-Risk Adult) Financial Exploitation or Abuse** – Any action which involves the misuse of an at-risk adult's funds or property.

1.1.8 **Third-Party Financial Exploitation** – Financial exploitation of an at-risk adult by another individual or party. The third party involved may be a caregiver, an individual with the power to act on behalf of the elder (Power of Attorney) or a service provider (e.g., a contractor).

1.1.9 **Executive Function** – An umbrella term for cognitive processes that regulate, control, and manage other cognitive processes, such as planning, working memory, attention, problem solving, verbal reasoning, inhibition, mental flexibility, multi-tasking, and initiation and monitoring of actions.

1.2 Legal Obligations

1.2.1 FinCEN Filings

1.2.1.1 February 2011 FinCEN Advisory

1.2.2 State Requirements

1.2.2.1 Institution's training should address, if applicable, specific legal state requirements, including Washington, DC.

1.3 Role of the Financial Institution

1.3.1 Help protect assets, mitigate losses and safeguard consumer information.

1.3.2 Report suspicious activities to FinCEN.

1.3.3 Report suspicious activities to local Adult Protective Services or law enforcement.

1.4 Stories of experiences

1.4.1 Provide examples of recent cases.

1.4.1.1 Family Fraud

1.4.1.2 Gold Investment Scheme

1.4.2 Reach out to local Area Agency on Aging or Adult Protective Services for examples.

1.4.3 Oklahoma Bankers Association "Senior Cents" Video

1.4.4 Oregon Bankers Association Video – uploaded to YouTube by California Bankers Association

2.0 Fraud Schemes[3]

2.1 Categories of Exploiters

[3] See *Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation* for more information on these scams.

2.1.1 People known to the victim (family members, friends, caregivers, or fiduciaries). The most common type of fraud with over 90% of cases according to the National Adult Protective Services Association.
- 2.1.1.1 Signing checks or documents without the victim's consent.
- 2.1.1.2 Charging excessive fees for rent or caregiver services.
- 2.1.1.3 Theft of money or property.
- 2.1.1.4 Obtaining money or property by undue influence, coercion, misrepresentation or fraud.
- 2.1.1.5 Power of Attorney abuse.

2.1.2 Strangers (scam artists, contractors, service providers)
- 2.1.2.1 Grandparent Scam
- 2.1.2.2 Telemarking Sweepstakes and lottery scams
- 2.1.2.3 Nigerian scams
- 2.1.2.4 Contractor/Home improvement fraud
- 2.1.2.5 Unsolicited work scam
- 2.1.2.6 Reverse mortgage proceeds scam
- 2.1.2.7 Bank examiner fraud
- 2.1.2.8 Mail fraud
- 2.1.2.9 Internet fraud
- 2.1.2.10 Phishing
- 2.1.2.11 Internet dating scam
- 2.1.2.12 "Pigeon drop" scam
- 2.1.2.13 Non-delivery of merchandise or payment
- 2.1.2.14 Overpayment
- 2.1.2.15 Advance fee scam
- 2.1.2.16 Affinity scams – military, cultural, religious

3.0 Suspicious behaviors

3.1 Visual Cues

3.1.1 New individual(s) accompanying the customer and overly interested in the account or encouraging a withdrawal.

3.1.2 Companion not allowing individual to speak for themselves or make decisions.

3.1.3 Individual appears nervous or afraid of the person accompanying them.

3.1.4 Secretive or giving implausible explanations for use of funds.

3.1.5 Unable to remember financial transactions or signing paperwork.

3.1.6 Isolated or inaccessible so the institution is unable to speak directly with the consumer.

3.1.7 Isolated from other family members or close friends.

3.1.8 Decline in physical appearance or lack of hygiene often indicates a neglected older adult who is at risk of becoming a victim.

3.1.9 Sudden appearance of previously uninvolved relatives claiming their rights to the consumer's affairs and possessions.
3.1.10 Excitement about winning a sweepstakes or lottery.
3.1.11 Excitement about a new soon to be delivered purchase.
3.1.12 Excitement about helping a new companion pay expenses to enter the country.

3.2 Transactional Cues
3.2.1 Unusual volume of activity.
3.2.2 Account activity inconsistent with at-risk adult's transaction history.
3.2.3 Suspicious signatures.
3.2.4 A fiduciary or other person (joint account holder) begins handling consumer's affairs and appears to be acting in self-interest or not in the best interest of the at-risk adult.
3.2.5 Statements and cancelled checks are no longer sent to the customer's home.
3.2.6 Change of address on accounts to new recipient's address – especially when distant from customer's home.
3.2.7 Abrupt changes to financial documents, such as power of attorney, account beneficiaries, wills and trusts, property title and deeds.
3.2.8 Unexplained disappearance of funds or valuable possessions, such as safety deposit box items.

4.0 In cases of suspected fraud or abuse
4.1 Verify the transactional authority of person(s) acting on the account holder's behalf.
4.2 Attempt to separate the account holder from the individual accompanying him or her.
4.3 Use probing open-ended questions to determine the consumer's intent.
4.4 Share an awareness document.
4.5 Delay the suspicious transaction, if possible.
4.6 Contact loss prevention and/or legal departments for assistance and guidance.

5.0 Role of the loss prevention department
5.1 Document the fact patterns.
5.2 Take protective action on accounts by placing holds or restraints.
5.3 Report the incident to law enforcement.
5.4 Verbal report to local Adult Protective Services.
5.5 Provide a written report. (required in California and Maryland)
5.6 Advise Customer contact staff on next steps.

6.0 Discussion of successful identification of perpetrator.

Additional Training for Fraud Investigators

7.0 Interview reporting employee.
7.1 Description and/or identification of perpetrator.
7.2 Document steps taken by the employee to prevent and respond.

8.0 Interview victim, if willing.
- 8.1 Description and/or identification of perpetrator and suspicious activity.
- 8.2 Record on video, if possible.

9.0 Collect and document surveillance videos and photos.

10.0 Completing a Suspicious Activity Report (SAR) for FinCEN.
- 10.1 Check the "other" box with a notation "elder financial exploitation".
- 10.2 Other relevant boxes may be checked if appropriate (i.e. wire fraud, identity theft, etc.).
- 10.3 In addition, the narrative section of the SAR should provide a detailed description of the violation of law or suspicious activity including any additional delivery channels used in the fraud and any additional fraudulent activities used to perpetrate the fraud.
- 10.4 Notify law enforcement contacts that a SAR has been filed.

11.0 Contacting appropriate agencies
- 11.1 Local Adult Protective Services
- 11.2 Eldercare Locator
- 11.3 Local law enforcement

12.0 State Compliance Requirements

13.0 Additional resources
- 13.1 American Bar Association's Commission on Law and Aging
- 13.2 Can Bank Tellers Tell?
- 13.3 Consumer Financial Protection Bureau's Office of Older Americans
- 13.4 National Adult Protective Services Association
- 13.5 National Center on Elder Abuse

Appendix A: For Senior Customers

Establish a budget. Identify all current obligations (e.g., mortgage payment, supplemental health insurance, prescription drugs). Identify all current sources of revenue. Determine the amount to spend each month and develop an appropriate budget.

Determine the appropriate products for you. Institutions offer a wide variety of products to respond to consumer needs. Investigate the products and determine which will benefit your lifestyle. Ask questions if you do not understand a product's features and make sure you understand any fees and, especially for investments, risks associated with the product before agreeing to purchase it. Your bank or financial institution or the local Area Agency on Aging can offer you educational information on financial products. Financial institutions offer resources to explain these.

Plan for your estate. To assist your family when decisions must be made, it is helpful to have the following legal documents: a durable power of attorney in the case of incapacity, living will for health care decisions, and a will for property distribution decisions. You should seek the assistance of a lawyer to complete these documents. If you cannot afford a lawyer, many communities offer free or low cost legal services for seniors.

Be ready for the unexpected. No one can predict when tragedy will strike, but all should plan accordingly. Establish an emergency fund with enough for three months' expenses.

Choose a trusted individual when providing power of attorney. Your attorney can discuss the benefits of appointing a power of attorney (POA) so someone can make decisions on your behalf when you are no longer able. Carefully review the authority the power of attorney document grants your designee, especially regarding the ability to perform financial transactions and give gifts. Ask your POA for periodic reports of the transactions they conduct on your behalf and ask to review your bank statements on a regular basis.

Stay active and engage with others regularly. Fraudsters prey on individuals who have infrequent contact with others. Stay active in your community. Most communities have senior centers that offer social activities.

Respond cautiously to in-person, mail, Internet or solicitations. No one should ask you to send them money unless you purchased or bought a product or service. Likewise, legitimate organizations offering contests or lotteries would never ask you to send them money to "claim your prize." Be cautious of any deal that sounds too good to be true. Discuss with a trusted friend or family member any request you get to send someone you do not know money. For instance, you can't win a lottery, if you haven't entered.

Know that wiring money is like sending cash. Con artists often insist that people wire money, especially overseas. If you wire money, it is nearly impossible to get your money back or trace the

money. Don't wire money or write checks to strangers, to sellers who insist on wire transfers for payment, or to someone who claims to be a relative in an emergency.

Contact your bank or financial institution if a request looks suspicious. Fraudsters may contact you claiming to be your bank or financial institution. Before providing any information, especially private information like your social security number, bank account numbers or passwords for your computer, contact your bank or institution through your regular channels (e.g., in-person visit, phone call to the bank's number listed on your bank statement) to confirm the request is from your bank or institution.

Protect your passwords and account numbers. Do not share your passwords and/or account numbers with others. If you think someone has obtained your password, immediately notify the institution.

Don't let embarrassment or fear keep you from discussing suspicious activities. We all make mistakes and often do not realize we have until after it has happened. If you think you have made a mistake with your finances, the situation could become worse if not escalated. Discuss any suspicious activity with someone you trust (e.g., family member, bank manager, attorney, local Area Agency on Aging, police).

Monitor your financial affairs. Actively track your financial accounts so you will be able to quickly recognize when a fraudulent transaction appears. Read your bank and credit card statements. Look for things that you did not authorize or do yourself. If you find suspicious activity, call your bank or credit card company immediately.

Check your credit report regularly. Checking your report can help you guard against identity theft. Visit http://www.ftc.gov/idtheft if you spot accounts that aren't yours. Visit www.AnnualCreditReport.com or call 1-877-322-8228, the only authorized website for free credit reports. You'll need to provide your name, address, Social Security number and date of birth to verify your identity.

Don't deposit checks you receive from strangers. Fraudsters may ask you to deposit a check and then require you to send a portion back. They do this to gather information about you that they then use to impersonate you. Ask your institution for help to prove the legitimacy of a check before you send any money to a stranger.

Keep details of all deals in writing. When making a financial decision always ask questions to ensure that you feel comfortable and confident where your money is going. Keeping a record of this information may help remedy a situation if the deal was in fact a fraud scam.

Look out for common scams. Criminals have similar tactics that they often use. These include posing as a repairman that you did not call, claiming to be a relative in emergency, or stating that you've won a sweepstakes or lottery that you did not enter.

Ask for assistance. Many financial institutions have programs specifically designed to help their customers. Beware of "advisors" claiming special qualifications and certifications to advise seniors. Contact your state securities regulator to check on specific licenses. In addition, credit counseling resources are available through the following:

National Foundation for Credit Counseling (NFCC)
1.800.388.2227
www.nfcc.org

The Federal Trade Commission (FTC)
www.ftc.gov/bcp/menus/consumer/credit/debt.shtm

Consumer Credit Counseling Service
1.800.388.2227
www.cccsatl.org

You can also contact your local Area Agency on Aging or call 1-800-677-1116.

Appendix B: For Family Members and Fiduciary

Discuss financial wishes. Before capacity is diminished, discuss financial plans with your elderly family member in a non-confrontational setting. Reassure him or her that you want to learn about their plans and concerns, not impose your own ideas upon them.

Learn about estate documents. These documents may include a will, durable power of attorney and health care proxy. It will be important that you know where these are stored in the event of an unfortunate circumstance. If the family member involved does not have these documents, encourage them to get them through a qualified attorney. If the family member cannot afford an attorney, many communities offer free or low cost legal services for seniors.

Act on behalf of the individual. When given the Power of Attorney, it is your fundamental responsibility to act in the best interest of the individual. You must use the elder's funds for the care of the elder. No funds should be used for your own desires.

Watch for signs of mental changes or abuse.

Diminished mental capacity

- Confusion over simple concepts; disorientation
- Failure to remember basic facts or recent conversations
- Difficulty performing simple tasks
- Drastic shifts in investment styles or investment objectives
- Unexplained withdrawals, wire transfers or other changes in financial situation
- Erratic behavior or dramatic mood swings
- Over-reliance on a third-party
- Inability to make decisions
- Diminished hearing
- Diminished vision
- Memory Loss

Third Party Financial Abuse

- Account withdrawals that are unexplained or not typical
- Inability to contact the vulnerable adult
- Signs of intimidation or reluctance to speak, especially in the presence of a caregiver
- Sudden or highly increased isolation from friends and family
- Checks written to strangers or to parties to whom the elder has never written a check
- Someone forging signatures
- Improper use of conservatorships, guardianships or powers of attorney

If you have been given power to act as a fiduciary, encourage the adult to review his or her bank and credit card statements regularly and consider reviewing them with the individual.

Appendix C: For Financial Institution Staff

Keep a record. When talking with any customer, it is important for the employee to keep all records as required by the institution. In cases of suspected fraud or abuse, the employee may want to note additional details.

Report suspected fraud or abuse to appropriate internal team. Institutions have internal compliance teams that will be able to assist in a suspected fraud or abuse case. The team will assist, as appropriate, with contacting the client's family, involving other third party professionals, reaching out to appropriate institution departments, and engaging adult protective services.

Verify the transactional authority of person(s) acting on the customer's behalf. As with any transaction, ensure that the individual has the legal authority to perform the transaction. In cases of an individual not associated with the account is with the consumer, separate the vulnerable adult from the individual accompanying him or her.

Use probing questions. Specific questions will help 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, when finalizing a power of attorney "Mr. Jones, do you want Ms. Smith to be able to withdraw money from your account at any time without needing your permission?" Or when someone accompanies an elder to your institution and you suspect the potential that the person is influencing the elder, you might privately ask, "Mr. Jones, are you sure you want to do this transaction?" and explain the effect of the transaction.

Share an awareness document. In cases where the consumer is suspected to be a potential victim of a fraud scheme, share awareness documents provided by the institution or others to help the consumer understand that the situation involved is a known fraud scheme. Organizations such as the Federal Bureau of Investigation have developed overviews of the most common schemes.

Watch for signs of mental changes or abuse.[4]

Diminished mental capacity

- Confusion over simple concepts; disorientation
- Failure to remember basic facts or recent conversations
- Difficulty performing simple tasks
- Drastic shifts in investment styles or investment objectives.
- Unexplained withdrawals, wire transfers or other changes in financial situation
- Erratic behavior or dramatic mood swings
- Over-reliance on a third-party
- Inability to make decisions

[4] Depending on the relationship of the customer with the employee will determine the inclusion of the following items. For example, financial advisors may have an increased ability to identify and report diminished capacity.

- Diminished hearing
- Diminished vision
- Memory loss

Third Party Financial Abuse

- Account withdrawals that are unexplained or not typical
- Inability to contact the vulnerable adult
- Signs of intimidation or reluctance to speak, especially in the presence of a caregiver or person accompanying the elder
- Isolation from friends and family
- Someone cashing checks without authorization
- Someone forging signatures
- Improper use of conservatorships, guardianships or powers of attorney