BITS

FINANCIAL SERVICES ROUNDTABLE

PROTECTING THE ELDERLY FROM FINANCIAL FRAUD AND EXPLOITATION

WHITE PAPER FOR THE ELDER JUSTICE COORDINATING COUNCIL

November 2, 2012

A PUBLICATION OF
BITS
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH WASHINGTON
DC 20004
(202) 289-4322
WWW.BITS.ORG

PROTECTING THE ELDERLY FROM FINANCIAL FRAUD AND EXPLOITATION

Table of Contents

Introduction 1
Role of the Financial Services Industry 2
Types of Abuse and Scams 3
Popular Scams 4
Relatives and Caregivers 6
Development of an Internal Awareness and Training Program 7
Program Design and Employee Training 7
Role of Customer Contact Staff 7
Role of Loss Prevention/Security 7
Role of Legal Departments 8
Role of Law Enforcement and Communities 8
Consumer Awareness and Education 8
Challenges and Impediments 9
Clarify the permissibility of age-based fraud monitoring 9
Authority to authorize a protective hold on a suspicious transaction 9
Power of Attorney Privileges Used for Inappropriate Transactions 9
Reporting of Suspicious Activities 10
Financial Literacy 11
Licensing of Financial Professionals Focused on Elderly Issues 11
Appendix A: Variations of Common Phishing and 419 Scams 12
Appendix B: Resources for Financial Institutions 14
Appendix C: Tips for Senior Consumers 20
Appendix D: Tips for Family Members and Fiduciary 22

INTRODUCTION

This paper, *Protecting the Elderly and from Financial Fraud and Exploitation*, is designed to address special needs for which financial institutions are uniquely suited to assist. The paper provides information to support the implementation or improvement of a financial institution's internal program for education and awareness about abuse of, and exploitation against, the elderly.

According to the National Center on Elder Abuse (NCEA), Bureau of Justice Statistics[1], 9.5% of the elderly population was abused in 2010. In a telephone survey[2] 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. The National Adult Protective Services Association (NAPSA) conducted an informal study of U.S. news articles regarding elder abuse reported between October 1, 2008 and March 31, 2009. Of the 1,971 incidents publicly reported, 458 of the incidents included financial exploitation[3]. A 2009 report estimates the annual financial loss by victims of elder financial abuse to be at least $2.6 billion. It also describes the typical victim of elder abuse as a woman over 75 who lives alone.[4]

By 2030, the number of Americans aged 65 and older will more than double to 71 million, roughly 20 percent of the U.S. population. In some states, fully a quarter of the population will be aged 65 and older[5]. This dramatic increase in the aging population can also lead to a large pool of potential victims for financial exploitation.

According to NCEA, financial exploitation can include "the illegal or improper use of an elder's funds, property, or assets." Examples include, but are not limited to, "cashing an elder adult person's 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 (e.g., contracts or will); and the improper use of conservatorship, guardianship, or power of attorney."[6]

Financial exploitation can be devastating to the victim. Research has shown that elders who suffer from abuse, neglect or exploitation are three times more likely to die than those who have not suffered from abuse, neglect or exploitation.[7] Compounding the devastation is that the exploitation is often traced to family members, trusted friends, or caregivers. Financial abuse often occurs with the implied acknowledgment and/or consent of the elder person, even when that person is mentally capable, and therefore can be more difficult to detect or prove. In addition, many victims may be unable or unwilling to implicate a friend or family member as the perpetrator. The University of

---

[1] *Bureau of Justice Statistics, http://bjs.ojp.usdoj.gov/*

[2] *March 2009 National Elder Mistreatment Study, http://www.ncjrs.gov/pdffiles1/nij/grants/226456.pdf.*

[3] Other categories tracked by NAPSA included physical, sexual, and emotional abuse, neglect (including self-neglect), abandonment, and information about scams, proposed legislation, community meetings, etc.

[4] Broken Trust: Elders, Family, and Finances, MetLife Mature Market Institute; produced in conjunction with the National Committee for the Prevention of Elder Abuse and Virginia Tech, *http://www.metlife.com/assets/cao/mmi/publications/studies/mmi-study-broken-trust-elders-family-finances.pdf.*

[5] *The State of Aging and Health in America,* Centers for Disease Control and Prevention (CDC) and The Merck Company Foundation, 2007, *http://www.cdc.gov/Aging/pdf/saha_2007.pdf.*

[6] The National Center on Elder Abuse, http://www.ncea.aoa.gov/ncearoot/Main_Site/index.aspx.

[7] Lachs, M.S., Williams, C.S., O'Brien, S., Pillemer, K.A., and Charlson, M.E., "The mortality of elder mistreatment" *Journal of the American Medical Association*, (1998) 280(5),428-432.

Chicago survey found that adults over the age of 60 are less likely to report verbal or financial mistreatment than those aged 50–60. According to the NCEA, Bureau of Justice Statistics, 15.7% of elder abuse cases reported in 2010 were cases of financial exploitation.

Why are older persons at risk? Greed is the major motivator of the perpetrator of the financial crime. Persons over 50 control the majority of the personal wealth in this country and the problem will only increase as the "baby boomer" generation ages. Fear is also a primary factor. Older adults are afraid of being left alone or being placed into a nursing home. The physical and mental impairments of aging make the elderly dependent on others for care, which allows the abuser to isolate and control the victim both physically and emotionally.

Employees within the financial services industry may often be the first to detect changes in the behaviors of customers with whom they have regular contact. This front-line relationship places institutions in a unique position to assist in protecting customers, upholding their inherent trust relationship with clients. Misconceptions and misunderstandings of privacy laws[8] may cause institutions to avoid reporting suspected financial exploitation even though many states mandate such reporting.

Financial institutions are encouraged to broaden dialogue with and report suspected fraud to Adult Protective Services (APS), as required by law[9]. In turn, APS will conduct investigations, prepare assessments and arrange for services needed to help victims correct or eliminate financial exploitation.

ROLE OF THE FINANCIAL SERVICES INDUSTRY

The financial services industry is uniquely positioned to assist in detecting and preventing financial fraud and exploitation of the elderly. Following are some of the reasons this role is critically important.

- A primary role of financial institutions is the protection of assets and prevention of financial losses. Experts from BITS member financial institutions develop and share best practices and other voluntary guidelines to safeguard consumer information.

- For decades, financial institutions have been at the forefront of fraud detection utilizing sophisticated technology, modeling, training and education, and are often the first to detect patterns of fraud. These proactive measures help to promote goodwill within the financial institutions' communities.

- Using a variety of safeguards, financial institutions ensure the reliability and security of financial transactions as well as protect financial privacy. While federal regulators require some of these

[8] See Role of Legal Departments section for more information.
[9] Currently, 20 states and the District of Columbia require financial institutions to report suspected cases of financial abuse of the elderly. To view your state's law, as well as state-specific data and statistics, statewide resources, etc., visit http://www.ncea.aoa.gov/NCEAroot/Main_Site/Find_Help/State_Resources.aspx. See also, http://www.ncea.aoa.gov/NCEAroot/Main_Site/Library/Laws/APS_IA_LTCOP_Citations_Chart_08-08.aspx, for the American Bar Association Commission on Law and Aging's list of state statutes.

safeguards, financial institutions often exceed the minimum standards of such regulation for the benefit of their customers, shareholders and employees.

- Financial institutions educate employees and customers on steps to secure accounts against the lure of fraudsters. Often, fraud is committed by trusted third parties, family or friends, and may be committed with the implied consent of the customer.

TYPES OF ABUSE AND SCAMS

NCEA recognizes six types of abuse[10]. In addition to signs of financial abuse, financial institution personnel may recognize, identify and report other forms of abuse. Identification of non-financial abuse may indicate that financial abuse is also occurring. The types of abuse below may be independent of each other:

- **Abandonment** – Desertion of an adult by an individual who has assumed responsibility for providing care.

- **Emotional or psychological abuse** – Trauma after exposure to threating acts or coercive tactics.

- **Financial abuse or exploitation** – Unauthorized or improper use of the resources of an elder for monetary or personal benefit, profit, or gain.

- **Neglect** – Failure to fulfill any part of a person's obligations or duties to an elder's physical, emotional, or social needs.

- **Physical abuse** – Injuring, assaulting or threatening with a weapon, or inappropriately restraining.

- **Sexual abuse** – Sexual contact against an elder's will.

Financial exploitation can be classified into two broad categories. These categories of exploitation may affect more than older consumers; however they are highlighted for purposes of understanding the direct risk they pose to the elderly.

- **Theft of income** – Most common form of financial exploitation and fraud. Theft is typically between $1,000 and $5,000 per transaction.

- **Theft of assets** – Often more extensive and typically involves abuse associated with Powers of Attorney, real estate transactions, identity theft or tax manipulation.

[10] These definitions are similar to those provided by the Centers for Disease Control (CDC), http://www.cdc.gov/ViolencePrevention/eldermaltreatment/definitions.html. The CDC and their partners are developing a document containing standardized definitions and recommended data elements for use in elder maltreatment public health surveillance. The updated document is expected to be released in late 2010.

Some forms of exploitation may be considered "scams," in which a person (or persons) unknown to the adult attempts to trick the victim for financial gain. The elderly person, who may be more trusting, gullible, or less financially sophisticated, are often the preferred targets of scams.

Popular Scams
The frauds outlined below are not unique to seniors, but the opportunity and impact can be greater than on the average consumer.

- **Advance Fee Fraud or "419" Fraud**. Named after the relevant section of the Nigerian Criminal Code, this fraud is a popular crime with West African organized criminal networks. There are a myriad of schemes and scams – mail, email, fax and telephone promises are designed to entice victims to send money for various reasons. Victims are told they will receive a percentage for their assistance.

  There are many variations of phishing and 419 schemes, but they all have the same goal: to steal the victims' money or personal and account information. *See Appendix A for more information about the various schemes.*

- **Debt Relief Scam** – Senior Americans are using their credit cards more to compensate for decreasing retirement portfolios and increasing medical costs,[11] and financially distressed elders may be susceptible to debt relief scams by unscrupulous companies that promise to repair a bad credit report or renegotiate a debt. Seniors may fall victim to companies that seek upfront fees for services that are often provided at little or no cost by the government. They may instruct the senior to redirect the payments to them, not the creditor, and either keep the payment entirely or charge exorbitant fees (sometimes 50%) as service charges. These companies often require payment in cash or money order, claiming that this decreases their overhead costs and keeps fees to a minimum, when it's actually done so the payments cannot be tracked like credit or debit card payments

- **Exploitation by a Financial Institution Employee** – While institutions go to great lengths to avoid hiring known fraudsters[12] and employ monitoring and access controls to prevent them from unnecessarily accessing customers' records, some employees may abuse their relationships or use their knowledge of internal processes to steal from their elderly customers.

- **Fictitious Relative** – The perpetrator calls the victim pretending to be a relative in distress and in need of cash, and asks that money be wired or transferred either into a financial institution account.

- **Financial Institution Examiner Impersonation Fraud** – The victim believes that he or she is assisting authorities to gain evidence leading to the apprehension of a financial institution employee or examiner that is committing a crime. The victim is asked to provide cash to bait the

[11] *The Plastic* Safety Net*: How Households are Coping in a Fragile Economy*, Demos, July 2009, http://www.demos.org/pubs/psn_7_28_09.pdf. The study reports that low- and middle-income consumers 65 and older carried $10,235 in average card debt in 2008, an increase in 26% from 2005,

[12] Many institutions perform background checks during the hiring process or screen names against the Internal Fraud Prevention Service which was developed by BITS and is maintained by Early Warning Services. For more information about the Internal Fraud Prevention Service, see http://www.earlywarning.com/human_resources.asp.

crooked employee. The cash is then seized as evidence by the "authorities" to be returned to the victim after the case.

- **Foreclosure Rescue Scam** – The perpetrator claims to be able to stop instantly foreclosure proceedings on the victim's real property. The scam often involves the victim deeding the property to the perpetrator who says that the victim will be allowed to rent the property until some predetermined future date when the victim's credit will have been repaired and the property will be deeded back to the victim without cost. Alternatively, the perpetrator may offer the victim a loan to bridge his or her delinquent payments, perhaps even with cash back. Once the paperwork is reviewed, the victim finds that his or her property was deeded to the perpetrator. A new loan may have been taken out with an inflated property value with cash back to the perpetrator, who is now the property owner. The property very quickly falls back into foreclosure and the victim, now tenant, is evicted.

- **Identity Theft** – Using one or more pieces of the victim's personal identifying information (including, but not limited to, name, address, driver's license, date of birth, Social Security number, account information, account login credentials, or family identifiers), a perpetrator establishes or takes over a credit, deposit or other financial account in the victim's name.

  Fraudsters gather victim's information through various means; however, senior citizens are often susceptible to social engineering techniques that fraudsters use, such as **"phishing"** to entice victims to supply personal information such as account numbers, login IDs, passwords, and other verifiable information that can then be exploited for fraudulent purposes. Phishing is most often perpetrated through mass emails and spoofed websites, but it can also occur through old-fashioned methods such as the phone, fax and mail.

- **Misappropriation of Income or Assets** – A perpetrator obtains access to an older consumer's Social Security checks, pension payments, checking or savings account, credit or ATM cards, and withholds portions of checks cashed for himself or herself.

- **Pigeon Drop** – A victim is approached by a stranger (or strangers) claiming to have found a large sum of money who offers to share it with the victim. However, the fraudster requests "good faith" money and offers to accompany the victim to the bank to withdraw the funds. In return, the victim is given an envelope or bag that contains blank pieces of paper rather than money.

- **Power of Attorney Fraud** – The perpetrator requests a Limited or Special Power of Attorney, specifying that legal rights be given to manage funds assigned for investment to the perpetrator, a trustee, an attorney, an asset manager, or other title that sounds official and trustworthy. Once the rights are given, the perpetrator uses the funds for personal gain.

- **Reverse Mortgage Scam** – Fraudsters may target senior citizens who have accumulated a sizeable amount of equity in their home. While there is nothing illegal with reverse mortgage products, the process can be complex and homeowners must carefully review all of the terms and conditions (preferably with family members and an attorney) before signing anything. Unscrupulous estate planners may charge fees for information that is available at no charge from

the U.S. Department of Housing and Urban Development (HUD)[13] or "mortgage consultants" may insist that unnecessary renovations must be done to the home in order to qualify for the loan and specify which contractor should be used to make these repairs.

- **Sweetheart Scam** – The perpetrator enters the victim's life as a romantic interest in order to gain influence and eventual financial control. This type of fraud often goes unreported due to the embarrassment and emotional impact on the victim. At times, the victim knows they are being duped but they simply do not want to be alone.

- **Telemarketing or Charity Scam** – The victim is persuaded to buy a valueless or nonexistent product, donate to a bogus charity, or invest in a fictitious enterprise. Seniors are particularly vulnerable to this type of fraud because they are often at home during the workday to answer the phone. Social isolation is also a factor where fraudsters prey on lonely seniors anxious for someone with whom to talk. They devise schemes that require multiple phone calls and development of a trusting relationship.

- **Unsolicited Work** – Victims are coerced, intimidated or otherwise conned into paying unreasonable amounts for poor quality work for services such as roofing, paving, auto body repair, etc. Often the work is fully paid for, but never started or of such poor quality that the victim must pay legitimate contractors to repair the work. Sometimes the work is only partially completed and the fraudster will insist that more money must be paid for the job to be completed. Often the perpetrator will accompany the victim to the bank to withdraw cash to pay for the substandard or incomplete work.

Relatives and Caregivers

Unlike strangers, relatives, caregivers, and others with fiduciary responsibilities, hold a position of trust and have an ongoing relationship with the older consumer. Financial exploitation occurs when the offender steals, withholds or otherwise misuses the victim's money or assets for personal profit. Perpetrators take advantage of the victim and rationalize their actions in various ways. For example, perpetrators may feel that they are entitled to receiving their inheritance early and do not view their actions as wrong, while others simply take advantage of the victim.

- **Borrowing money** (sometimes repeatedly) with no intent to repay.

- **Cashing or keeping some portion** of the person's pension, Social Security or other income checks without permission.

- **Opening or adding their name to banking accounts** without the elder's permission. Often, a fraudster may use the victim's personal information to open an account online, as opposed to opening an account at a branch location. The fraudster often opts to receive online statements to avoid having statements sent to the victim's address and elude detection.

- **Theft of the victim's money or other cash-equivalent assets** (e.g., stocks, bonds, savings bonds, travelers checks), both directly and through establishing joint accounts or signatory authority on existing accounts. Perpetrators may convince the elder to add them to the account

[13] http://www.hud.gov/offices/hsg/sfh/hecm/hecmhome.cfm.

as an authorized user without the elder understanding that the perpetrator can withdraw funds without their knowledge.

- **Transferring title on, or re-encumbering, real property** of the older consumer. Financial exploitation utilizing real property is particularly appealing to family members or caregivers who may feel they are "owed" something for their efforts, however meager those efforts may be in reality. For many elderly, their most significant economic asset may be the equity they have built in their real property over decades of ownership.

- **Using the victim's checks or ATM, debit or credit cards** without permission.

The tactics used by these offenders may include intimidation, deceit, coercion, emotional manipulation, psychological or physical abuse and/or empty promises. The offender may try to isolate the victim from friends, family and other concerned parties who would act in the victim's best interest. By doing so, the perpetrator prevents others from asking about the person's well-being or relationship with the offender and prevents the person from consulting with others on important financial decisions.

DEVELOPMENT OF AN INTERNAL AWARENESS AND TRAINING PROGRAM

Financial institutions understand the importance of establishing and internal awareness and training program on this issue. Most institutions train all of their staff on this issue when they are hired, and then perform regular trainings for those individuals who work directly with consumers. This section outlines the responsibility of each part of an institution in combating this abuse.

Program Design and Employee Training

Corporate support is important when developing and maintaining a successful awareness and training program. Institutions should involve and seek input not only from their internal departments, but also from external groups such as protective services and law enforcement, as they often have a keen understanding regarding the cases and issues affecting a specific region.

Role of Customer Contact Staff

Customer contact staff are in a unique position to identify potential abuse of elder populations through greater awareness and recognition of "red flags" in customer behavior. The industry is in the process of establishing an overview of curriculum for training customer facing personnel to identify potential signs of fraud. This work will include identifying key "red flags" that staff may identify during routine account servicing that could indicate actual or potential fraud.

Role of Loss Prevention/Security

Loss prevention/security staff are strongly encouraged to proactively contact and establish relationships with local law enforcement and APS offices to increase collaboration and information sharing with these groups before an incident occurs.

In addition, the regional field offices of the Federal Bureau of Investigation (FBI) and U.S. Secret Service (USSS) sponsor task forces that serve as an excellent means to network and share

information regarding crimes affecting the region. Local FBI[14] or USSS[15] field offices will be able to direct an institution to the a local task force.

Role of Legal Departments

Financial institutions may be reluctant to report suspicious activity to APS due to concerns with federal and state privacy laws. According to the American Bar Association (ABA) Commission on Aging, The Right to Financial Privacy Act of 1978 applies only to federal agencies requesting consumer information from financial institutions. Further, the 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." In addition, 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 laws.

In 2003, the ABA published the document, *Can Bank Tellers Tell? Reporting Financial Abuse of the Elderly*,[16] which outlines state laws associated with elder abuse. Another paper, *Legal Issues Related to Bank Reporting of Suspected Elder Financial Abuse*[17] provides an overview of the legal issues that institutions may consider when reporting suspected cases of financial exploitation of the elderly.

As stated above, financial institutions should consult with legal departments on the specific reporting guidelines for the states in which they do business. In some cases, a written request from APS is sufficient to release customer statements and transaction copies, while other states require a subpoena or written consent from the customer.

Role of Law Enforcement and Communities

National Organization of Triads (NATI) is a partnership of law enforcement, senior citizens and community groups to promote senior safety and reduce the unwarranted fear of crime that the elder community often experiences. A handbook[18] is available to assist law enforcement and senior citizens in implementing a comprehensive crime prevention program for older adults.

CONSUMER AWARENESS AND EDUCATION

Consumer education is critical to preventing fraud. Most individuals will take action if they believe it will decrease their chances of being victimized by fraud, as long as the action does not significantly inconvenience them. By educating customers, financial institutions can decrease fraud losses.

Included in the *Appendix* are resources institutions may refer customers for tips on preventing fraud. Institutions can share this information with customers through various channels, such as postings at the branches, flyers sent with monthly statements, emails, through a Web site, and/or by request to a call center.

---

[14] List of FBI field offices, http://www.fbi.gov/contact/fo/fo.htm.
[15] List of the USSS field offices, http://www.secretservice.gov/field_offices.shtml.
[16] http://www.ncea.aoa.gov/ncearoot/main_site/pdf/publication/bank_reporting_long_final_52703.pdf
[17] http://www.ncea.aoa.gov/ncearoot/main_site/pdf/publication/bank_reporting_summary_final_52703.pdf
[18] http://www.nationaltriad.org/tools/Draft_Triad_Handbook.pdf

CHALLENGES AND IMPEDIMENTS

While financial institutions recognize the importance and their responsibility in protecting older customers from fraud and abuse, there areas that require an increased focus to more effectively respond to these threats.

Clarify the permissibility of age-based fraud monitoring

Financial institutions utilize sophisticated fraud detection technology and modeling in their attempts to prevent and identify potential fraudulent activity to protect customers. An added layer of scrutiny for older customers' activities, could identify more efficiently identify abnormalities in transactions. However, providing additional security to these specific accounts could place a financial institution in violation of existing age discrimination laws and, therefore, put the institution at risk for potential fines or regulatory actions.

The Department of Justice should review this issue and clarify permissibility of age-based fraud monitoring. A written opinion of the permissibility would be extremely helpful. If, in fact, it is considered a violation of current anti-discrimination laws to segregate this population for fraud monitoring purposes.

Authority to authorize a protective hold on a suspicious transaction

If an employee strongly suspects or knows the older consumer has fallen for a scam, but the elderly customer wants to perform a transaction (e.g., a withdrawal, a request to transfer funds), the institution is contractually obligated to carry out the customers instructions. In these cases, institutions may try to convince the consumer that the transaction is in response to a fraudulent request, but they may be unsuccessful.

The Consumer Financial Protection Bureau and Treasury should create an option allowing institutions to put a minimal hold on the transaction pending the sending of an alert of APS and APS discussing the situation with the customer.

The U.S. Department of Justice, U.S. Postal Inspection Service, Federal Trade Commission and other agencies along with input from financial institutions should create and maintain a list of known fraudulent actors that can be used to "convince" elders of their involvement in a fraudulent situation. By providing documentation to an older consumer from a trusted source in the government, individuals may be more easily understand that they are the victim of the fraud.

A shareable database of local and regional APS services, as well as, contacts at the Area Agency on Aging would more easily identify for institutions who to contact in discussing these types of situations with involved elders. Along with creating a database for contacts, it will be necessary to clarify further the type of information institutions are legally able to share with APS regarding their older customer.

Power of Attorney Privileges Used for Inappropriate Transactions

Similar the situation described of a victim wanting to go through with a transaction after they have been told that it could be fraud, individuals with a Power of Attorney have the ability to perform transactions on the older consumers behalf. If a financial institution suspects that they are trying to perpetrate fraudulent activity or activity not in the best interest of the elder. Duly executed Powers of Attorney give the holder the legal right to act on behalf of the customer.

Powers of Attorney laws and regulations vary by state and, particularly in the case of Durable Powers of Attorney, can involve granting rights to the agent even after the principal becomes incapacitated. While the agent is obligated to exercise due care and protect the principal, state law is not uniform with respect to the specific responsibilities of an agent with regard to financial transactions, particularly when the principal is an elder. The development of uniform state laws and a Uniform Power of Attorney would be very helpful. Study of the feasibility and benefits of having a uniform Power of Attorney, particularly one for situations in which the principle is an elder should be undertaken.

Select agencies – most likely U.S. Department of Health and Human Services, Social Security Administration, CFPB, U.S. Department of Justice, the Federal Trade Commission and the U.S. Department of Veterans Affairs – should consider working collaboratively to develop educational materials that explain clearly to those agents with Powers of Attorney their financial responsibilities and provide specific examples of what are considered abusive behaviors.

The U.S. Department of Justice could undertake a study of existing criminal statutes that apply to financial abuse of elders. This should include both federal and state level statutes with the goal to develop a model criminal code applicable to this area that strongly disincents criminal actors and those acting as agents from taking advantage of the elderly.

Reporting of Suspicious Activities

Financial institutions are sometimes concerned with the liability they or their employees might incur in situations where they suspect and report elder abuse – particularly if it is a situation in which it is ultimately determined that a fraud was not involved. Today, certain states require the reporting of even suspicions of fraud, but that reporting is not uniform on a national level and statutory hold harmless provisions to protect the reporter seem far from consistent.

The Council should work toward legislative action that would result in a national reporting statute that provides uniform electronic reporting requirements to a single report point which would disseminate the information (or otherwise make it available) to state and local agencies, as well as uniform hold harmless protections for reporting parties. Additionally, the importance of federal and state agencies such as the CFPB, SEC, FINRA, and NSAA, etc., to coordinate their efforts in addressing elder financial abuse can ensure the avoidance of conflicting rules and regulations, which themselves would potentially harm individual clients. This should also include a definition of those individuals who are protected by the requirements, as in some states fraud of vulnerable adults follow the same requirements as fraud of the elderly.

FinCEN, a part of the U.S. Treasury, issued an advisory on February 22, 2011 that addresses the reporting of actual or suspected elder financial abuse on Suspicious Activity Reports (SARS). This provided financial institutions with guidance on reporting specific to SARs' requirements; however, the reporting of elder financial abuse often goes beyond that type of reporting. Reporting would likely include reporting of situations to Adult Protective Services or similar agencies as well potentially, depending on the circumstances, to local law enforcement. Today, however, the structure of adult protective services type agencies is diffused across the country. Some locations have more centralized statewide or regional agencies will others structure such agencies very locally. Determining the correct agency for reporting is often difficult. Law enforcement capabilities to deal with such reports often vary as well. In addition, today with law enforcement often done at the local

level, it is often difficult to synthesize information across jurisdictions to identify when elders in different locations may be being subjected to scams and fraudulent activity that relates to the same set of criminal actors.

Recognizing that local law enforcement lacked skills in investigating cybercrime, in 2007, the Department of Homeland Security, the United States Secret Service, the Alabama District Attorneys Association, the State of Alabama, and the city of Hoover, Alabama partnered to create the National Computer Forensics Institute (NCFI). This partnership provides state and local law enforcement officers the training necessary to conduct basis electronic crimes investigations. Creating a similar model to train state and local law enforcement personnel the training necessary to conduct investigations of elder abuse could have significant merits. Short of such a large effort, creating and providing to local law enforcement bodies an educational opportunity through such options as written best practices, webinars and seminars on the subject would be beneficial.

Note that these same concepts can be generally applied as well to local prosecutorial authorities, who sometimes also lack the knowledge and experience requisite to the successful prosecution of those who prey financially on the elderly. Similar training programs and best practices can also serve this community well.

While SARS reporting is working well today, a significant improvement can be made by specifically adding "Elder Financial Abuse" as a category in Section 35 of the SARs Reporting Form. This would allow for easier collation of such activity and facilitate cross matching of potential criminal actors within this area.

Financial Literacy

Enhanced financial literacy further empowers consumers, including older Americans, to make sound financial decisions. Financial literacy is one of the highest priorities for the Roundtable and its members at the grass roots and at the national policy level. In 2011, Roundtable member companies conducted more than 45,600 financial literacy projects around the country to empower further thousands of consumers to make sound financial decisions.

The Roundtable is currently in the process of developing a structure for training financial institution consumer-facing employees. In addition, the Roundtable is developing a publicly available awareness and education program to be made available to all financial institutions for adoption or modification.

A national-level awareness campaign targeting elder Americans and their family members would provide long-lasting benefits in helping to reduce elder financial abuse.

Licensing of Financial Professionals Focused on Elderly Issues

In the Roundtable's August 20, 2012 letter to the CFPB regarding CFPB's "Request for Information Regarding Senior Financial Exploitation [Docket CFPB-2012-0018]," the Roundtable mentioned another key area to reduce financial abuse of elders. It noted that an effort to make elders more aware of the licensing of financial professionals coupled with an effort by federal and state agencies and professional organizations' role in developing best practices for the training and licensing of financial professionals would have benefits.

APPENDIX A: VARIATIONS OF COMMON PHISHING AND 419 SCAMS

- **Inheritance scams** – Victims receive mail from an "estate locator" or "research specialist" purporting an unclaimed inheritance, refund or escheatment. The victim is lured into sending a fee to receive information about how to obtain the purported asset.

- **Internet sales or online auction fraud** – The perpetrator agrees to buy an item available for sale on the Internet or in an online auction. The seller is told that he or she will be sent an official check (e.g., cashier's check) via overnight mail. When the check arrives, it is several hundred or thousand dollars more than the agreed-upon selling price. The seller is instructed to deposit the check and refund the overpayment. The official check is subsequently returned as a counterfeit but the refund has already been sent. The seller is left with a loss, potentially of both the merchandise and the refund.

- **Recovery Room Scams** – Fraudsters build lists of consumers who have previously fallen victim to a scam and sell them to telemarketers. These "sucker lists" contain detailed information about the victim including the name, address, phone number and information about money lost in the scam. The telemarketers contact the victims, often posing as government agents, and offer–for a fee–to assist the victim in recovering the lost money. The consumer is often victimized twice, as a government or consumer advocacy agency would not charge a victim for this assistance.

- **Work-from-Home Scams** – Potential employees are recruited through newspaper, email and online employment services for jobs that promise the ability to earn money while working from the comfort of home. However, many customers unwittingly become mules for fraudsters who use their accounts to launder money or even steal from them. For example, a customer may apply for a position as a "mystery shopper," "rebate processor," "trading partner," or a "currency trader." Upon being hired, the new "employee" provides their bank account information to their employer or establishes a new account using information provided by the employer. The employee is instructed to wire money that is deposited into the accounts to drop boxes via Western Union. Rather than processing rebates or trading currency, the customer is actually participating in a money-laundering scheme where the fraudsters use the employee's (mule's) legitimate account to transfer stolen money to other accounts out of the country.

- **International lottery and sweepstakes fraud** – Scam operators, often based in Canada, use telephone and direct mail to notify victims that they have won a lottery. To show good faith, the perpetrator may send the victim a check. The victim is instructed to deposit the check and immediately send (via wire) the money back to the lottery committee. The perpetrator will create a "sense of urgency," compelling the victim to send the money before the check, which is counterfeit, is returned. The victim is typically instructed to pay taxes, attorney's fees and exchange rate differences in order to receive the rest of the prize. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail. In a similar scam, victims are advised that they are the winner of a sweepstakes. However, they do not receive their initial "winnings" but are encouraged to write small dollar checks in order to get them to the next round to win a larger sweepstakes prize.

- **Fake prizes** – A perpetrator claims the victim has won a nonexistent prize and either asks the person to send a check to pay the taxes or obtains the credit card or checking account number to pay for shipping and handling charges.

- **Charitable donation scam** – Scam artists claiming to represent charitable organizations use e-mails and telephone calls to steal donations and in some cases donors' identities.

- **Government grant scams** – Victims are called with the claim that the government has chosen their family to receive a grant. In order to receive the money, victims must provide their checking account number and/or other personal information. The perpetrator may electronically debit the victim's account for a processing fee, but the grant money is never received.

- **Spoofing** – An unauthorized website mimics a legitimate website for the purpose of deceiving consumers. Consumers are lured to the site and asked to log in, thereby providing the perpetrator with authentication information that the perpetrator can use at the victim's legitimate financial institution's website to perform unauthorized transactions.

- **Pharming** – A malicious Web redirect sends users to a criminal's spoofed site even though the user entered a valid URL in the browser's address bar. This redirection usually involves worms and Trojans or other technologies that attack the browser address bar and exploit vulnerabilities in the operating systems and Domain Name Servers (DNS) of the compromised computers.

- **Home Stealing** – Using public records to obtain information about property records and property transfer forms purchased at any office supply store, fraudsters may use false identification, forge the true property owner's signature and transfer the deed without the true owner's knowledge. Many states do not require deed recorders or those who oversee property closings to authenticate the identities of buyers or sellers who submit the information filed with the city or county recorder's office. These "stolen homes" are often used as collateral for new loans or sold to cash-paying buyers at a fraction of the property's value. The buyers themselves are often victims of this scam as they are unaware that the property was hijacked from the true owner.

- **Investment Property** – Property is sold to the elderly consumer as a guaranteed investment with high yield returns. The victim is convinced to buy investment property through, or in conjunction with, a property management firm that will handle all the loan documents, make all the loan payments, place the tenants, collect the rents and maintain the property. The victim is told that he or she has to do nothing other than be the buyer and borrower. The property then falls into foreclosure. The victim finds that the property was inflated in value, payments at the closing were made to the property management company or affiliated parties, no loan payments have ever been made, and any collected rents have been stolen as well.

AGENCIES AND ASSOCIATIONS

Department of Health and Human Services
Administration on Aging (AoA)
Washington, DC 20201
Ph: (202) 619-0724
Fax: (202) 357-3555
Email: aoainfo@aoa.hhs.gov
http://www.aoa.gov

National Adult Protective Services Association (NAPSA)
920 S. Spring Street, Suite 1200
Springfield, IL 62704
Ph: (217) 523-4431
Fax: (217) 522-6650
http://apsnetwork.org

National Center on Elder Abuse (NCEA)
c/o Center for Community Research and Services
University of Delaware
297 Graham Hall
Newark, DE 19716
Email: ncea-info@aoa.hhs.gov
http://www.ncea.aoa.gov
Resources by State:
http://www.ncea.aoa.gov/NCEAroot/Main_Site/Find_Help/State_Resources.aspx

National Center for Victims of Crime
2000 M Street NW, Suite 480
Washington, DC 20036
Ph: (202) 467-8700
Fax: (202) 467-8701
Email: gethelp@NCVC.org
http://www.ncvc.org
A helpline is staffed Monday through Friday 8:30am to 8:30pm EST:
Toll-free Helpline: 1-800-FYI-CALL (1-800-394-2255)
TTY/TDD: 1-800-211-799

National Organization of Triads, Inc. (NATI)
1450 Duke Street
Alexandria, VA 22314
Ph: (703) 836-7827
Fax: (703) 519-8567
Email: nati@sheriffs.org
http://www.nationaltriad.org

Identity Theft Assistance Center (ITAC)
ITAC, the Identity Theft Assistance Center, is a nonprofit founded by The Financial Services Roundtable as a free service for consumers. Since 2004, ITAC has helped more 60,000 consumers recover from identity theft by giving them a single point of contact to identify and resolve suspicious account activity. ITAC shares victim data with law enforcement agencies to help investigate and prosecute identity crime and forms partnerships on identity theft education and research initiatives. Through its partner Intersections Inc., ITAC offers the ITAC Sentinel® identity management service (www.itacsentinel.com). For more information visit http://www.identitytheftassistance.org.

TRAINING MATERIALS AND TOOLKITS

Attorney General of Texas – Senior Texans Page – Texas has launched a statewide outreach campaign to raise awareness for protecting senior Texans. More information can be found at the Texas Attorney General website: http://www.oag.state.tx.us/elder/index.shtml

Clearinghouse on Abuse and Neglect of the Elderly (CANE) – CANE is a collaborator in the National Center on Elder Abuse (NCEA), which is funded by the Administration on Aging, U.S. Department of Health and Human Services. CANE identifies a comprehensive list of resources on the many facets of elder mistreatment. Visit www.cane.udel.edu for more information.

The Elder Consumer Protection Program – The program, housed at Stetson University College of Law's Center for Excellence in Elder Law, serves as a progressive and evolving educational, informational, and instructional resource, to both professionals and the public, on general and legal topics regarding current and developing issues, matters, and concerns in the area of elder consumer protection. The Program, which is supported in part by state and federal funding, offers assorted materials and various services that provide and promote general knowledge, public awareness and assistance, and professional development and training. Materials and services include, but are not limited to, speeches and presentations, brochures and handouts, web page platforms and interfaces, non-legal consumer inquiry assistance, reference databases, and resource guides. Details and additional information can be found at http://www.law.stetson.edu/elderconsumers.

Elder Financial Protection Network (EFPN) – The Network works to prevent financial abuse of elders and dependent adults through community education programs, public awareness campaigns and coordination of financial institution employee training. Financial institution statement stuffers, brochures and posters can be ordered via the website at http://bewiseonline.org.

Elder Abuse Training Program – Developed in conjunction with the Oregon Department of Human Services, this 2-hour educational curriculum teaches professional and family caregivers about the complexities of domestic elder abuse and neglect. More information on this program, including cost, can be found at: http://www.medifecta.com/.

Federal Bureau of Investigation (FBI) – The FBI offers a free fraud alert poster, available at http://www.fbi.gov/majcases/fraud/fraud_alert.pdf, for placement in branches to help alert customers to common check fraud scams. The FBI's site also provides information about common fraud schemes and those targeting senior citizens. For more information, see http://www.fbi.gov/majcases/fraud/fraudschemes.htm or http://www.fbi.gov/majcases/fraud/seniorsfam.htm.

Fiduciary Abuse Specialist Team (FAST) – The Los Angeles FAST team was developed to provide expert consultation to local APS, Ombudsman, Public Guardian and other caseworkers in financial abuse cases. The team includes representatives from the police department, the district attorney's office, the city attorney's office private conservatorship agencies, health and mental health providers, a retired probate judge, a trust attorney, an insurance agent, a realtor, an escrow officer, a stockbroker, and estate planners. The FAST coordinator and consultants have also provided training to bankers and police officers across the state of California. They have developed a manual and have

helped other communities start up FAST teams. For more information, visit http://www.preventelderabuse.org/communities/fast.html.

Financial Institution Elder Abuse Training Kit – Developed in 1995 and updated in 2007 in conjunction with the Oregon Department of Human Services, this kit also includes videos, manuals and other materials. For more information contact:

Oregon Bankers Association
777 13th Street SE, Suite 130
Salem, OR 97301
or
PO Box 13429
Salem, OR 97309
Ph: (503) 581-3522
Fax: (503) 581-8714
http://www.oregonbankers.com/community/efapp

The Massachusetts Bank Reporting Project: An Edge Against Elder Financial Exploitation – The Massachusetts' Executive Office of Elder Affairs, in collaboration with the Executive Office of Consumer Affairs, and the Massachusetts Bank Association, developed the bank reporting project to provide training to bank personnel in how to identify and report financial exploitation, as well as foster improved communication and collaboration between the financial industry and elder protective services. The project has been successfully replicated in numerous communities. Sample materials, including model protocols, procedures for investigating and responding to abuse, and training manuals are available. For more information contact:

Jonathan Fielding
One Ashburton Place, 5th Floor
Boston, MA 02108
Ph: (617) 222-7484
Fax: (617) 727-9368
Email: jonathan.fielding@state.ma.us

Missouri Department of Health and Human Services – Missourians Stopping Adult Financial Exploitation (MOSAFE) Project – The MOSAFE website includes training materials for financial institution employees to help spot the warning signs of financial exploitation, and take steps to stop it. The materials include a video, brochure, PowerPoint presentation, resource manual, and eight articles, which can be viewed and/or downloaded from this site.
http://www.dhss.mo.gov/MOSAFE/index.html

National Center on Elder Abuse (NCEA) Training Library – In response to the needs of various agencies for training materials on elder abuse, neglect, and exploitation, the NCEA developed this national resource library. Technical assistance is provided to library users both on what is available through the library and on how to select the right materials to meet the user's particular needs. Most of the library's materials are now available for downloading. To learn more and access the library, visit:
http://www.ncea.aoa.gov/NCEAroot/Main_Site/Library/Training_Library/About_Training_Library.aspx

CONSUMER RESOURCES

AARP Foundation – In conjunction with the Colorado Attorney General the AARP Foundation has created the Colorado ElderWatch Project (http://www.aarpelderwatch.org/) to fight the financial exploitation of older Americans through collection of data.

Attorney General of Texas – Senior Texans Page – Texas has launched a statewide outreach campaign to raise awareness for protecting senior Texans. More information can be found at the Texas Attorney General website, http://www.oag.state.tx.us/elder/index.shtml

Federal Bureau of Investigation (FBI) – This FBI site includes information about common fraud schemes and those targeting senior citizens. For more information, see http://www.fbi.gov/majcases/fraud/fraudschemes.htm or http://www.fbi.gov/majcases/fraud/seniorsfam.htm.

Federal Deposit Insurance Corporation (FDIC) – The Federal Deposit Insurance Corporation publishes the FDIC Consumer News quarterly to help people protect and stretch their money. The Fall 2005 edition of "Fiscal Fitness for Older Americans: Stretching Your Savings and Shaping Up Your Financial Strategies" included a section on frauds targeting the elderly. For more information, see http://www.fdic.gov/consumers/consumer/news/cnfall05/index.html.

Federal Trade Commission (FTC) – The Federal Trade Commission's Bureau of Consumer Protection provides free information to help consumers detect and avoid fraud and deception. For more information, visit http://www.ftc.gov/bcp/index.shtml.

The FTC also operates a call center for identity theft victims where counselors tell consumers how to protect themselves from identity theft and what to do if their identity has been stolen (1-877-IDTHEFT [1-877-438-4338]; TDD: 1-866-653-4261; or http://www.ftc.gov/idtheft).

Identity Theft Assistance Center (ITAC) – ITAC is a nonprofit supported by financial services companies as a free service for their customers. ITAC shares information with law enforcement to help them investigate and prosecute fraud and identity theft. For a list of ITAC member companies and consumer information on identity theft detection and prevention, visit http://www.identitytheftassistance.org.

MetLife Mature Market Institute® (MMI) – The MMI site offers pamphlets, guides and tip sheets designed to assist decision-makers about retirement planning, caregiving and healthcare. Such publications include *Helpful Hints: Preventing Elder Financial Abuse*[19] and *Preventing Elder Abuse.*[20] For more information about other guides, reports, and resources offered by the MMI, visit www.maturemarketinstitute.com.

North American Securities Administrators Association, Inc (NASAA) – The North American Securities Administrators Association (NASAA) is an international organization devoted to investor protection. The NASAA Fraud Center,

---

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

[20] Since You Care guides, http://www.metlife.com/mmi/publications/since-you-care-guides/index.html

http://www.nasaa.ar/Investor Education/NASAA Fraud Center/, contains resources and information to protect against investor fraud.

APPENDIX C: TIPS FOR SENIOR CONSUMERS

Establish a budget. Identify all current obligations (e.g., mortgage payment, supplemental health insurance, prescription drugs). 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 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 make gifts.

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 cannot win a lottery, if you have not entered.

Know that wiring money is like sending cash. Con artists often insist that people wire money, especially overseas, because it is nearly impossible to get your money back or trace the money. Do not 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 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.

Do not let embarrassment or fear keep you from discussing suspicious activities. We all make mistakes and often do not realize we have until after we have. 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 recognize quickly 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 activity you did not do, call your bank or credit card company immediately.

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

Do not 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 repairperson that you did not call for, claiming to be a relative in emergency and stating that you have won a sweepstakes or lottery that you did not enter.

Ask for assistance. Many financial institutions have programs specifically designed to help. 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 1.800.388.2227 www.nfcc.org	The Federal Trade Commission 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 D: TIPS FOR FAMILY MEMBERS AND FIDUCIARY

Discuss financial wishes. Before capacity is diminished, discuss financial plans with your family members 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 older 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

About BITS

BITS 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. BITS is the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Roundtable member companies provide fuel for America's economic engine, accounting directly for $92.7 trillion in managed assets, $1.2 trillion in revenue, and 2.3 million jobs. For more information, go to http://www.bits.org/.

About The Financial Services Roundtable

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 $85.5 trillion in managed assets, $965 billion in revenue, and 2.3 million jobs.