

BITS

FINANCIAL SERVICES
R O U N D T A B L E

PROTECTING THE ELDERLY AND VULNERABLE FROM FINANCIAL FRAUD AND EXPLOITATION

February 2010

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

**PROTECTING THE ELDERLY AND VULNERABLE FROM
FINANCIAL FRAUD AND EXPLOITATION**

TABLE OF CONTENTS

<u>Introduction</u>	3
<u>Role of the Financial Services Industry</u>	5
<u>Types of Abuse and Scams</u>	6
<u>Development of an Internal Awareness and Training Program</u>	11
<u>Working with State and Federal Agencies</u>	16
<u>Consumer Awareness and Education</u>	17
<u>Appendix</u>	
<u>A: Variations of Common Phishing and 419 Scams</u>	18
<u>B: Resources For Financial Institutions</u>	20
<u>Agency and Association Contacts</u>	20
<u>Training Materials and Toolkits</u>	22
<u>C: Consumer Resources</u>	24
<u>Acknowledgements</u>	25

INTRODUCTION

This paper, *Protecting the Elderly and Vulnerable 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 and vulnerable (vulnerable adults). For purposes of this paper, vulnerable adults includes those either over the age of 60–65, depending on the state, or disabled individuals over the age of 18. Often, vulnerable adults lack the physical or mental capability to care for themselves.

According to a 2008 survey by the University of Chicago¹, approximately 13 percent of elderly Americans have been verbally mistreated (9%) or financially exploited (3.5%) or have had advantage taken of them. In a telephone survey² 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. A 2001 study by the National Association of Adult Protective Service Administrators (NAPSA) reported 38,015 documented cases of financial exploitation of vulnerable adults. The study also states that only one out of 14 cases of domestic elder abuse incidences is reported, which could mean that numbers of cases of abuse exceed 850,000 annually. 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 exploitation³. 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 older⁵. This dramatic increase in the aging population can also lead to a large pool of potential victims for financial exploitation

According to the National Center on Elder Abuse (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 a vulnerable 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

¹ This study was based on a 2005–2006 survey by the National Social Life, Health and Aging Project (NSHAP) that collected data from a random sample of 3,005 community-dwelling adults aged 57–85. The study was supported by the National Institutes of Health (NIH) and published in the *Journal of Gerontology: Social Sciences*.

² *March 2009 National Elder Mistreatment Study*, <http://www.ngjrs.gov/pdf/files1/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/saba_2007.pdf.

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

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 Chicago survey found that adults over the age of 60 are less likely to report verbal or financial mistreatment than those aged 50–60.

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. A pilot program instituted by a financial institution to identify and detect cases of financial abuse of the elderly showed that in 7 out of 10 cases when a teller suspected something was wrong, they were correct. 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 laws⁸ may cause institutions to avoid reporting suspected financial exploitation even though many states mandate such reporting. A July 2003 NAPSA survey found that financial institutions accounted for only 0.3% of reports of financial exploitation⁹.

Financial institutions are encouraged to broaden dialogue with and report suspected fraud to Adult Protective Services (APS), as required by law¹⁰. In turn, APS will conduct investigations, prepare assessments and arrange for services needed to help victims correct or eliminate financial exploitation. This is an area in which they may make a positive contribution to the well-being of vulnerable customers.

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.

⁸ See Role of Legal Departments section for more information.

⁹ “State Adult Protective Services Program Responses to Financial Exploitation of Vulnerable Adults,” NAPSA, July 2003, http://www.ncea.aoa.gov/NCEARoot/Main_Site/pdf/publication/NAAPSA_9.pdf.

¹⁰ 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.

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 and vulnerable. Following are some of the reasons this role is so 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 some of these safeguards are required by federal regulators, financial institutions often exceed the minimum standards of such regulation for the benefit of their customers, shareholders and employees. In some states financial institutions are mandated to report instances of abuse or financial exploitation and in 49 states they are provided immunity from civil or criminal liability if acting in good faith in such reporting.
- 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. The ability to detect changes in behavior places financial institutions in a unique position to assist in protecting customers and uphold the inherent trust relationship with their clients.

TYPES OF ABUSE AND SCAMS

NCEA recognizes seven types of abuse¹¹. 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:

- **Self-neglect** – Failure by oneself to provide goods or services essential to avoid serious threat to one’s physical or mental health.
- **Neglect** – Failure to fulfill any part of a person’s obligations or duties to an elder. Neglect can be willful/intentional (e.g., deliberately withholding food or medicine) or unintentional (e.g., untrained or “burnt out” caregiver).
- **Physical abuse** – Infliction of physical pain, injury, etc.
- **Sexual abuse** – Non-consensual sexual contact of any kind with a vulnerable adult.
- **Abandonment** – Desertion of a vulnerable adult by an individual who has assumed responsibility for providing care.
- **Emotional or psychological abuse** – Infliction of mental anguish by demeaning name calling, threatening, isolating, etc.
- **Financial or material exploitation** – Illegal or unethical exploitation by using funds, property, or other assets of a vulnerable adult for personal gain irrespective of detriment to the vulnerable adult.

Financial exploitation can be classified into two broad categories. These categories of exploitation may affect more than vulnerable adults, however they are highlighted for purposes of understanding the direct risk they pose to the vulnerable:

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

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

¹¹ 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.

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

- **Power of Attorney fraud** – The perpetrator requests a Limited or Special Power of Attorney, specifying that legal rights are 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.
- **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 scam 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 don’t want to be alone.
- **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.
- **Exploitation by a financial institution employee** – While institutions go to great lengths to avoid hiring known fraudsters¹² 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.
- **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 crooked employee. The cash is then seized as evidence by the “authorities” to be returned to the victim after the case.
- **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.
- **Misappropriation of income or assets** – A perpetrator obtains access to a vulnerable adult’s Social Security checks, pension payments, checking or savings account, credit or ATM cards, and withholds portions of checks cashed for themselves.

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.

- **Foreclosure rescue scam** – The perpetrator claims to be able to instantly stop 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.
- **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.
- **Debt relief scams** – Senior Americans are using their credit cards more to compensate for decreasing retirement portfolios and increasing medical costs,¹⁴ 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 these 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
- **Telemarketing or charity scams** – 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 work day to answer the phone. Social isolation is also a factor where fraudsters prey on lonely seniors anxious for someone to talk to. They devise schemes that require multiple phone calls and development of a trusting relationship.
- **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.

¹³ <http://www.hud.gov/offices/hsg/sfh/hecm/hecmhome.cfm>.

¹⁴ *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,

- **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.

- **Advance fee fraud or “419” frauds.** 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, ostensibly to bribe government officials involved in the illegal conveyance of millions outside the country. Victims are to 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.

Financial institutions should train staff to be especially alert to suspicious activities and transactions involving their older customers and continue to ask the fundamental question, “Does it make sense for *this* customer to be conducting *this* transaction?” They should also look for signs that senior customers have been threatened or unduly influenced.

Relatives and Caregivers

Unlike strangers, relatives, caregivers, and others with fiduciary responsibilities, hold a position of trust and have an ongoing relationship with the vulnerable adult. 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. Methods can include:

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

- **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. 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 vulnerable adults, their most significant economic asset may be the equity they have built in their real property over decades of ownership. *See also foreclosure rescue scam.*
- **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.

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

This section is intended to serve as recommendations for financial institutions to consider when creating awareness and detection programs to protect their elderly and vulnerable customers from fraud and financial exploitation. Additional resources are located in [*Appendix B*](#).

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.

- Internal Sources:
 - Branch Administration
 - Loss Prevention/Security Department
 - Legal
 - Compliance
 - Public/Community Relations
 - Training

- External Sources:
 - Adult Protective Services (APS)/Department of Social Services
 - Local and/or State and Federal Law Enforcement
 - Local and/or State Prosecutorial Authorities (e.g. Attorneys General, District Attorneys)

BITS has developed a presentation deck that can be use to train financial institution employees. Contact Heather Wyson, heather@fsround.org, for more information.

Role of Customer Contact Staff

Customer contact staff are in a unique position to identify potential abuse of vulnerable populations through greater awareness and recognition of “red flags” in customer behavior. Below are “red flags” that staff may identify during routine account servicing that could indicate actual or potential fraud. Individually, these indicators are not problematic; however, further investigation is warranted if multiple red flags are present.

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.

Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation

- 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.
- 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.

Changes in Checking and/or Credit/Debit Spending and Transaction Patterns

- 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 checking or credit account or a new joint account.
- Account use shortly after the addition of a new authorized signer.
- 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.
- 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.
- 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.

Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation

- 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.

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.
- 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.

If you “**suspect fraud**” with your vulnerable adult customer:

- 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.
- 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. Examples include:
 - *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 419scam*: “Mrs. Green, \$4,000 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.”
- If your customer has asked for a large cash withdrawal which appears out of pattern, consider developing an “awareness” document for the consumer to read prior to receipt of funds. This could include:
 - Brief overviews of common fraud schemes. See *Types of Abuse and Scams* and *Appendix A* for more information,

Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation

- Warnings that perpetrators of such schemes could present themselves as an FBI agent, financial institution examiner, police officer, detective or financial institution official.
 - Warning that customers should use caution if they are asked for information about their account, or asked to withdraw money to help “catch someone,” or provide money to show “good faith.”
 - Notice that the financial institution does not conduct investigations or verification of accounts by telephone (since swindlers often use this method to gain information on accounts, as well as the confidence of their victims) nor will local, state or federal law enforcement authorities, financial institution regulatory authorities, or financial institution officials conduct investigations by asking individuals to withdraw cash from their account for any reason.
 - Phone numbers for the appropriate agencies, if any of the circumstances listed above are present, with instructions to customers that they should contact their branch, local police department, Adult Protective Services, or the Federal Trade Commission to investigate before they withdraw money.
 - Reminders that swindlers nearly always are friendly and have “honest” faces, and that they particularly tend to take advantage of older individuals.
- 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.

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. Contact your local FBI¹⁵ or USSS¹⁶ field office to determine if a task force is established in your region.

When abuse is suspected, staff are encouraged to:

- 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.

¹⁵ List of FBI field offices, <http://www.fbi.gov/contact/fo/fo.htm>.

¹⁶ List of the USSS field offices, http://www.secretservice.gov/field_offices.shtml.

- 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 as needed.¹⁷ 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. To locate the APS office that serves the customer, call 1-800-677-1116 or use their web database located at <http://www.eldercare.gov/Eldercare.NET/Public/Home.aspx>.
- Continue to monitor the account during legal proceedings, if necessary.
- Advise customer contact staff and appropriately document files of final outcome.

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*,¹⁸ which outlines state laws associated with elder abuse. Another paper, *Legal Issues Related to Bank Reporting of Suspected Elder Financial Abuse*¹⁹ 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.

The 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 handbook²⁰ is available to assist law enforcement and senior citizens in implementing a comprehensive crime prevention program for older adults.

¹⁷ If you suspect elder abuse, neglect or exploitation, visit the National Center on Elder Abuse's State Elder Abuse Helplines and Hotlines Web page to find out where to report it.

¹⁸ http://www.ncea.aoa.gov/ncearoot/main_site/pdf/publication/bank_reporting_long_final_52703.pdf

¹⁹ http://www.ncea.aoa.gov/ncearoot/main_site/pdf/publication/bank_reporting_summary_final_52703.pdf

²⁰ http://www.nationaltriad.org/tools/Draft_Triad_Handbook.pdf

WORKING WITH STATE AND FEDERAL AGENCIES

Adult Protective Services (APS)

The role of APS, which operates under state law in every state, is to receive and investigate reports of vulnerable adult abuse, and offer services when the abuse is confirmed. APS confidentially investigates each case, making contact with and interviewing the customer. If financial abuse is confirmed, steps are taken to eliminate the abuse. APS also often works with legal service providers to offer protection to victims through the legal system and with law enforcement and the criminal justice system to prosecute those responsible for abuse. While financial institutions are often the first to identify suspected fraud and in turn contact APS directly, APS may also be notified by other external sources.²¹ When this occurs, APS contacts financial institutions to assist in confirming the fraud. If the financial institution is the abuse reporter, APS will, if allowable under state law, advise the financial institution of the final determination. Furthermore, APS works to educate the elderly and vulnerable community as well as others of the problems facing consumers. APS also promotes the development of needed legislation and public policy.

U.S. Administration on Aging (AoA)²²

The Administration on Aging was created by the Older Americans Act (OAA), originally signed into law by President Lyndon B. Johnson on July 14, 1965. The Act authorized grants to states for community planning and services programs, as well as for research, demonstration, and training projects in the field of aging. Later amendments to the Act added grants to local agencies on aging for local needs identification, planning, and funding of services, including nutrition programs in communities as well as for those who are homebound; programs to serve native American elders; health promotion and disease prevention activities; in-home services for frail elders; and services to protect the rights of older persons.

AoA supports two programs that specifically promote the rights of seniors and protect them from exploitation. AoA coordinates these programs at the national level, and members of the Aging Network implement them at the State and local level. The goal of the *Elder Abuse, Neglect, and Exploitation Prevention Program* is to develop and strengthen prevention efforts at the State and local level. This includes funding for State and local public awareness campaigns, training programs, and multi-disciplinary teams. The State Legal Assistance Development Program is another essential element in protecting elder rights under Title VII of the Older Americans Act. The Act is one of the top funding sources for low-income senior legal assistance. Nationwide, approximately 1,000 legal services providers funded through the Act provide more than one million hours of assistance to seniors per year on a wide range of legal issues, including predatory lending, investment schemes, identity theft, home repair scams, and other types of financial exploitation.

To augment and enhance these consumer protection efforts, AoA funds a number of other projects. The National Center on Elder Abuse (NCEA) is a gateway to resources on elder abuse, neglect, and exploitation. Among its activities, NCEA makes available news and materials; provides consultation, education, and training; answers inquiries and requests for information; and operates a listserv forum for professionals. NCEA also facilitates the exchange of strategies for uncovering and

²¹ Many professionals, including bankers in about 20% of states, are mandated to report suspected vulnerable adult abuse to APS.

²² For more information on all of AoA's consumer protection efforts, please visit the Elder Rights section of the AoA website, http://www.aoa.gov/AoARoot/AoA_Programs/Elder_Rights/index.aspx.

prosecuting fraud in areas such as telemarketing and sweepstakes scams, and has produced a number of telemarketing fraud alert and elder fraud alert newsletters. For more information, see <http://www.ncea.aoa.gov>.

The AOA also provides funding for the National Legal Resource Center (NLRC), which provides tools to legal services providers to help older adults facing the most difficult challenges to their independence and financial security. Through the NLRC, legal and aging services providers receive intensive case consultation and training on complex and emerging issues in law and aging, technical assistance in the efficient, cost effective and targeted provision of legal services, and access to other informational resources. Major topics of focus include consumer credit, bankruptcy, debt collection, unfair and deceptive practices, sales and warranties, foreclosure prevention, energy assistance, and public utility practices. NCLC has several products related to older consumer fraud available on their website, http://www.consumerlaw.org/initiatives/seniors_initiative/.

In addition, AOA has supported special projects like the Philadelphia APS-Wachovia collaboration and the Stetson University Consumer Protection Education Project. These projects developed collaborations between APS, law enforcement, banks, and other community members to identify, prosecute, and prevent fraud and financial exploitation of seniors.

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.

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 vulnerable adult 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.

APPENDIX B: RESOURCES FOR FINANCIAL INSTITUTIONS

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://bewiseline.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 case workers 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 stock broker, 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 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*²³ and *Preventing Elder Abuse*.²⁴ 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, http://www.nasaa.org/Investor_Education/NASAA_Fraud_Center/, contains resources and information to protect against investor fraud.

²³ <http://www.metlife.com/assets/cao/mmi/publications/consumer/mmi-helpful-hints-preventing-elder-financial-abuse-olderadults.pdf>

²⁴ Since You Care guides, <http://www.metlife.com/mmi/publications/since-you-care-guides/index.html>

ACKNOWLEDGMENTS

This paper was originally published by BITS in February 2006 and amended in 2009 to include updated statistics and information about new or evolving scams.

We would like to acknowledge and thank those who participated in the development of this revised document:

Linda Mill, Financial Exploitation Training and Investigations Specialist
Joe Snyder, Philadelphia Corporation for Aging

BITS Member Companies

Stacy Barber, BBVA Compass
Cindy Enslin, BBVA Compass
Vivian Richardson, BBVA Compass
Teresa Steele, BBVA Compass
Dianne Shovel, Comerica Incorporated
Jeffrey Bloch, CUNA
Lin Collier, CUNA/VyStar Credit Union
Dorothy Steffens, CUNA
Danette LaChappelle,
CUNA/ICQ Credit Union
Danielle Jamiot, Fifth Third Bancorp
Dilip Chemburkar, Genworth Financial
Karen Trimmer, JPMorgan Chase & Co.

Stacy Bennett, RBC Bank, USA
Tom Backstrom, Sovereign Bancorp
Stephanie Whittier, U.S. Administration on Aging
Omar Valverde, U.S. Administration on Aging
Deborah Broderick, US Bancorp
Mitchell Lincoln, USAA
Nathan Wolf, USAA
Sandy Jalicke,
Wells Fargo & Co./Wachovia Bank
Deborah Ronan,
Wells Fargo & Co./Wachovia Bank
Luana Tafoya,
Wells Fargo & Co./Wachovia Bank

About BITS

BITS is the technology policy division of The Financial Services Roundtable, created to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS focuses on strategic issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services by leveraging intellectual capital to address emerging issues at the intersection of financial services, operations and technology. BITS' efforts involve representatives from throughout our member institutions, including CEOs, CIOs, CISOs, and fraud, compliance and vendor management specialists. 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 \$74.7 trillion in managed assets, \$1.1 trillion in revenue, and 2.3 million jobs. For more information, go to <http://www.fsround.org/>.

