

BITS

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

BITS FRAUD PROTECTION TOOLKIT PROTECTING THE ELDERLY AND VULNERABLE FROM FINANCIAL FRAUD AND EXPLOITATION

FEBRUARY 2006

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

**BITS FRAUD PREVENTION TOOLKIT
PROTECTING THE ELDERLY AND VULNERABLE FROM
FINANCIAL FRAUD AND EXPLOITATION**

TABLE OF CONTENTS

Introduction	3
Role of the Financial Services Industry	5
Types of Abuse and Scams	6
Development of an Internal Awareness and Training Program	12
Working with State and Federal Agencies	17
Consumer Awareness and Education	19
About The BITS Fraud Reduction Program and BITS	20
Appendix of Resources and Recommendations to Consumers	21

INTRODUCTION

This *BITS Fraud Prevention Toolkit: 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 *Toolkit* provides information to support the implementation or improvement of a financial institution internal program for education and awareness about abuse of, and exploitation against, the elderly and vulnerable (vulnerable adults). For purposes of this *Toolkit*, 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.

The 1998 National Elder Abuse Incidence Study found that Adult Protective Services (APS) agencies substantiate more cases of financial abuse than they do of physical abuse each year and that only one in five cases of abuse, neglect and exploitation is reported to authorities. While these data are relatively old, there is no evidence that they are outdated, particularly in proportion to incidents of physical abuse and particularly in an aging society.

More current, the 2001 study by the National Association of Adult Protective Service Administrators (NAAPSA) 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.

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.”¹

Financial exploitation can be devastating to the victim. 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.

The financial services industry often may be the first to detect changes in the behaviors of customers with whom they have regular contact. This places institutions in a unique position to assist in protecting customers, upholding their inherent trust relationship with clients. Misconceptions and misunderstandings of privacy laws may cause institutions to avoid reporting suspected financial exploitation even though many states mandate such reporting. The National Adult Protective Services Association (NAPSA) July 2003 survey

* “Elder Mistreatment: Abuse, Neglect and Exploitation in an Aging America” 2003, Washington, DC: National Research Council Panel to Review Risk and Prevalence of Elder Abuse and Neglect

¹ The National Center on Elder Abuse (<http://www.elderabusecenter.org/default.cfm?p=basics.cfm>)

found that financial institutions accounted for only 0.3% of reports of financial exploitation.**

Financial institutions are encouraged to broaden dialogue and report suspected fraud to Adult Protective Services (APS). In turn, APS will conduct investigations, prepare assessments and arrange for services needed to help victims correct or eliminate financial exploitation. Financial institutions are not responsible for monitoring for the potential financial exploitation of customers, however, this is an area in which they may make a positive contribution to the well-being of vulnerable customers.

This *Toolkit* was developed by BITS. BITS is a non-profit industry consortium whose members are 100 of the largest financial institutions in the United States. The CEOs of The Financial Services Roundtable established BITS in 1997. BITS is the strategic business and technology division for The Financial Services Roundtable and works on key issues where industry cooperation serves the public good, such as critical infrastructure protection and the safety of financial services. Major purposes for BITS are to develop and disseminate industry best practices for improving information security programs, reducing fraud, managing third party providers, managing risk and fostering innovation. BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Advisory Board and BITS Advisory Council. For more information, go to www.bitsinfo.org.

** “State Adult Protective Services Program Responses to Financial Exploitation of Vulnerable Adults,” NAPSA, July 2003

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 the BITS financial institution members develop and share best practices and other voluntary guidelines to safeguard consumer information.
- Financial institutions have for decades 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 of financial institutions 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 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 abuse. 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 or 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.
- **Psychological abuse** – Infliction of mental anguish by demeaning name calling, threatening, isolating, etc.
- **Financial abuse** – 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 less than \$1,000 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 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. There are numerous variations, all of which are not attempted to be represented below. These scams, which may also affect the general public, include, but are not limited to:

- **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.

- **Phone company scam** – While pretending to be a representative from a local phone company, the perpetrator purports that a problem exists on the telephone line. The perpetrator asks the victim to call back under the guise of conducting a test. This allows the perpetrator to make long distance phone calls and bill them to the victim.
- **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.
- **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 facilitate victims’ parting with 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.
- **Pigeon drop** – The victim puts up "good faith" money in the false hope of sharing the proceeds of an apparent large sum of cash or item(s) of worth which are "found" in the presence of the victim.
- **Financial institution examiner 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.
- **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.
- **Financial institution employee fraud** – The perpetrator calls the victim pretending to be a security officer from the victim’s financial institution. The perpetrator advises the victim that there is a system problem or internal investigation being conducted. The victim is asked to provide his or her Social Security number for “verification purposes” before the conversation continues. The number is then used for identity theft or other illegal activity.
- **Itinerant fraud** – Victims are coerced, intimidated or otherwise conned into paying unreasonable amounts for poor quality work. Door-to-door solicitations occur where perpetrators offer services such as roofing or paving, auto body repair, etc. Often the work is fully paid for, but only partially completed, never started or of such poor quality that the victim must pay legitimate contractors to repair the work.

- **International lottery 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.
- **Misappropriation of income or assets** – A perpetrator, often a family member or caregiver, obtains access to a vulnerable adult's Social Security checks, pension payments, checking or savings account, credit card or ATM, or withholds portions of checks cashed for an elder adult.
- **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 (“account”) in the victim’s name.
- **Telemarketing scams** – The victim is persuaded to buy a valueless or nonexistent product, donate to a bogus charity or invest in a fictitious enterprise.
- **Fictitious relative** – The perpetrator calls the victim pretending to be a relative in distress and in need of cash and asks that money be transferred either into a financial institution account or wired.
- **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.
- **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.
- **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.

- **Unsolicited work** – A perpetrator arrives unexpectedly at a residence and offers to perform work for a reasonable fee. After starting the work, the perpetrator insists that the victim pay more than originally agreed before the work will be completed.
- **Phishing** – Technology or social engineering is used 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, including identity theft. Phishing is most often perpetrated through mass emails and spoofed websites.
- **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.
- **Stop Foreclosure 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.
- **Investment Property** – Property is sold to the vulnerable 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.

Relatives and Caregivers

Unlike strangers, relatives and caregivers 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. Methods can include:

- **Theft of the victim's money or other cash-equivalent assets** (e.g., stock, bonds, savings bonds, travelers checks), both directly and through establishing joint accounts or signatory authority on existing accounts.
- **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 ATM, debit or credit card** 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.

The tactics used by these types of offenders may include intimidation, deceit, coercion, emotional manipulation, psychological 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.

According to the Missouri Department of Health and Senior Services (DHSS) Division of Senior and Disability Services², **the top 10 "red flags"** associated with scams include:

1. Signature seems forged, unusual, or suspicious.
2. A set of "out-of-sync" check numbers.
3. Allegations of "missing funds" from a vulnerable adult's account.
4. A vulnerable adult fails to understand recently completed transactions or repercussions of his or her actions.
5. Financial institution or credit card statements start being sent to an address other than the vulnerable adult's home.
6. Unusual cash withdrawals from a checking account in a short period of time.

² Missouri Department of Health and Senior Services (DHSS) Division of Senior and Disability Services is available at <http://www.dhss.mo.gov/MOSAFE/index.html>.

7. Abrupt increase in credit card activity or a sudden flurry of “bounced” checks.
8. Vulnerable adult's account shows ATM activity even though he or she is physically unable to leave home.
9. Vulnerable adult is accompanied by a third party who encourages the withdrawal of a large sum of cash and may not allow the vulnerable adult to speak.
10. Abrupt and unexplained change in a financial Power of Attorney; new names added to signature cards; new joint account.

DEVELOPMENT OF AN INTERNAL AWARENESS AND TRAINING PROGRAM

The following outline is intended as a guide for use by financial institutions when creating awareness and detection programs to protect the elderly and vulnerable from fraud and financial exploitation.

Program Design and Employee Training

- Internal Sources:
 - Branch Administration
 - Loss Prevention/Security Department
 - Legal
 - Compliance
 - Public Relations
 - Training
- External Sources:
 - Adult Protective Services (APS)
 - Local and/or State Law Enforcement
 - Local and/or State Prosecutorial Authorities (e.g. Attorneys General, District Attorneys)

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. Signs of abuse or financial exploitation of vulnerable adults include, but are not limited to:

- 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.
- Recent changes in authorized signers on a vulnerable adult's financial institution signature card, particularly additions.
- Withdrawals of funds using an ATM card, particularly repetitive withdrawals over a short period inconsistent with prior usage patterns or at times, or on days, that appear unlikely to have been done by the customer (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 use of an ATM card which was only recently ordered commensurate with the addition of a new authorized signer).
- Abrupt changes in a will or other financial documents.
- Unexplained disappearance of funds or valuable possessions.

- Substandard care being provided or bills unpaid despite the apparent availability of adequate financial resources.
- Discovery of a vulnerable adult's signature being forged for financial transactions or for the titles of his or her possessions.
- Sudden appearance of previously uninvolved relatives claiming their rights to a vulnerable adult's affairs and possessions.
- Vulnerable adult has a companion who seems to be “calling the shots.”
- Vulnerable adult has no knowledge of newly-issued ATM, debit or credit card.
- Vulnerable adult is confused about the account balance or transactions on his or her account.
- A caregiver appears to be getting paid too much or too often.
- Significant increases in monthly expenses being paid from an account (which may indicate that expenses for persons other than the customers are being paid).
- Request for a new Power of Attorney that the vulnerable adult does not appear to understand.
- Vulnerable adult reports concerns about giving out personal and account information to a solicitor via the phone or email.
- Unexplained sudden transfer of assets, particularly real property, to a family member or someone outside the family.
- Excitement about winning a sweepstakes or lottery.
- Provision of services that are not necessary.
- A vulnerable adult's report of financial exploitation³.
- Sudden appearance of credit card balances with no prior history of using credit.
- Change in the vulnerable adult's appearance (hair or clothes disheveled or lack of hygiene).

³ The National Center on Elder Abuse (<http://www.elderabusecenter.org/default.cfm?p=basics.cfm>)

- 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.

What to do if you “**suspect fraud**” with your vulnerable adult customer:

- Carefully verify anyone’s authority 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 tell you 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 419 scam*: “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 an “awareness” document, and potentially ask the customer to sign it prior to receipt of funds. The form could include:
 - Brief overviews of common fraud schemes.
 - 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 about are in evidence, 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.
 - The amount the individual has requested, with a request to read and sign the document.
- 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.
 - Report the incident to law enforcement following your institution’s normal protocol.

Role of Loss Prevention/Security

- 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.
- Make a verbal report to the local APS and provide investigative research and services as needed. 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 ww.eldercare.gov/Eldercare/Public/Home.asp.
- Continue to monitor the account during legal proceedings, if necessary.
- Advise customer contact staff and 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 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 the state's privacy law.

In 2003 the American Bar Association published the document, "Can Bank Tellers Tell? Reporting Financial Abuse of the Elderly," which outlines state laws associated with elder abuse. A link to the paper is provided in the appendix of this document. Note: The ABA is currently revising the document to bring it up to date with changes in the law. It is expected to be released early in 2006.

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

Triads – This 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. Tools for creating triads can be found at <http://www.nationaltriad.org>.

WORKING WITH STATE AND FEDERAL AGENCIES

Adult Protective Services (APS)

The role of APS is to receive and investigate reports of vulnerable adult abuse, and offer services when the abuse is confirmed. APS works with legal service providers to offer protection to victims through the legal system and with 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. When this occurs, APS contacts financial institutions to assist in confirming the fraud. Further APS works to educate the elderly and vulnerable community and beyond of the problems facing consumers. APS also promotes the development of needed legislation and public policy. APS confidentially investigates each case, making contact with and interviewing the customer. If financial abuse is confirmed, steps are taken to eliminate the abuse. Further, law enforcement may be contacted. If the financial institution is the abuse reporter, APS will advise the financial institution of the final determination.

U.S. Administration on Aging (AoA)

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.

Efforts to protect seniors' financial security from fraud, scams, and exploitation support AoA's primary goal of keeping seniors independent in their homes and communities. AoA administers formula grants for state activities designed to protect seniors, such as to train law enforcement officials and other professionals, develop and distribute educational materials, conduct public awareness campaigns, and create community coalitions. Formula grants to states also fund approximately 1,000 OAA legal services providers nationwide who serve low-income seniors. These legal providers help older Americans and their caregivers to address threats to home ownership such as predatory lending and consumer scams, and to obtain financial powers of attorney or guardianships that can prevent or stop 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 prosecuting fraud in areas such as telemarketing

and sweepstakes scams, and has produced a number of telemarketing fraud alert and elder fraud alert newsletters (www.elderabusecenter.org).

The AoA also provides funding for the National Consumer Law Center (NCLC), one of five National Legal Resource Centers, to improve the quality and accessibility of legal assistance for vulnerable older Americans with consumer problems. Major topics of specialization at the NCLC 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 supports 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 of Resources and Recommendations to Consumers** are resources to assist institutions with communicating to customers as well as a list of consumer tips to prevent 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.

THE BITS FRAUD REDUCTION PROGRAM

The BITS Fraud Reduction Steering Committee was created to:

- Reduce payment-related fraud losses.
- Secure a critical mass of financial institutions to participate in a shared account database and standardized data collection process.
- Identify successful strategies for reducing check fraud and make those strategies available to the industry.
- Assess fraud risk exposure to electronification and develop strategies to minimize losses.

Working Groups under the BITS Fraud Reduction Program include:

- Debit Card/ATM Fraud
- Electronification
- Emerging Fraud Risks
- Identity Theft
- Internet Fraud
- Prevention of the Exploitation of the Elderly and Vulnerable
- Shared Databases

This Toolkit was created with the assistance and expertise of Linda Mill, Senior Vice President, Wachovia, Joe Snyder, Director-Older Adult Protective Service, Philadelphia Corporation for Aging, and Brandt Chvirko, Aging Services Program Specialist, U.S. Administration on Aging. Please contact Robin Slade, Senior Consultant, at rmslade@sbcglobal.net for more information.

About BITS

BITS (www.bitsinfo.org) was created in 1996 to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. A nonprofit industry consortium that shares membership with The Financial Services Roundtable, BITS seeks to sustain consumer confidence and trust by ensuring the security, privacy and integrity of financial transactions. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS' activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Advisory Board and BITS Advisory Council.

APPENDIX OF RESOURCES AND RECOMMENDATIONS TO CONSUMERS

RESOURCES

AGENCIES AND ASSOCIATIONS

National Center on Elder Abuse (NCEA)
1201 15th Street, NW, Suite 350
Washington, DC 20005
Ph: (202) 898-2586
Fax: (202) 898-2583
Email: ncea@nasua.org
<http://www.elderabusecenter.org>

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

National Adult Protective Services Association (NAPSA)
1900 13th Street
Suite 303
Boulder, CO 80302
Ph: (720)-565-0906
Fax: (720)-565-0438
<http://apsnetwork.org>

TRAINING MATERIALS AND TOOLKITS

California Banker's Website includes training materials on elder abuse, including a free training video, which can be downloaded at:
http://www.calbankers.com/content/education_trainingmaterial.asp.

Financial Institution Elder Abuse Training Kit developed in conjunction with the Oregon Department of Human Services. Includes videos, manuals and other materials. For more information contact:
Marilyn Muller
Senior & Disabled Services Division
Abuse Prevention Unit
P.O. Box 14750
Salem, OR 97309
503-378-2529

Elder Financial Protection Network (EFPN): 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, is a 2-hour educational curriculum that 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.homecarecompanion.com/eatp.html>.

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>

Stetson University Consumer Protection Education Project: developed an elder consumer protection education program to educate elder consumers, their families, law enforcement, and other professionals about consumer fraud and how to minimize the risk of becoming victims. In addition to community presentations and educational programs, they have created a series of PowerPoints for presentations and re-enactment videos to show elders how various scams work. These PowerPoints and scam videos will be available beginning January 2006. Details and contact information can be found at <http://elder.law.stetson.edu/professional/>."

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, the Attorney General's Elderly Protection Project, and the Massachusetts Bank Association, developed the bank reporting project to provide training to bank personnel in how to identify and report financial exploitation. 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.

Contact:
Gillian Price
One Ashburton Place, 5th Floor
Boston, MA 02108
(617) 727-7750 ext. 222
(617) 727-9368 (fax)

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, extensive outreach and education, a free hotline for the elderly, and the provision of technical assistance. Training materials for financial institutions located in Colorado is also available at:
http://www.aarpelderwatch.org/public/training/before_the_money_is_gone.pdf

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.

Contact:

Rena R. Fountain-MSG
Director of Elder Abuse Prevention Program
WISE Senior Services
1527 Fourth Street, Ste 250
Santa Monica, CA 90401
(310) 394-9871

www.wiseseniors.org

Federal Bureau of Investigation (FBI) – free fraud alert poster can be placed in branches to help alert customers. The poster can be found at <http://www.fbi.gov/becrimesmart.htm>.



The poster features a background of scattered US dollar bills. At the top right is the FBI seal. The main title "FBI FRAUD ALERT" is in large, bold, red letters. Below it, a warning in black text asks if the reader can answer "YES" to any of the following questions, indicating they might be involved in a fraud or about to be scammed. A list of ten questions follows, each with a red circular icon. At the bottom, a green banner urges readers to tell branch personnel immediately. On the left side, a vertical blue banner with yellow text says "DON'T GET RIPPED OFF!".

FBI FRAUD ALERT

IF YOU CAN ANSWER "YES" TO ANY OF THE FOLLOWING QUESTIONS, YOU COULD BE INVOLVED IN A FRAUD OR ABOUT TO BE SCAMMED!

- Is the CHECK from an item you sold on the Internet, such as a car, boat, jewelry, etc?
- Is the amount of the CHECK more than the item's selling price?
- Did you receive the CHECK via an overnight delivery service?
- Is the CHECK connected to communicating with someone by email?
- Is the CHECK drawn on a business or individual account that is different from the person buying your item or product?
- Have you been informed that you were the winner of a LOTTERY, such as Canadian, Australian, El Gordo, or El Mundo, that you did not enter?
- Have you been instructed to either "WIRE", "SEND" OR "SHIP" MONEY, as soon as possible, to a large U.S. city or to another country, such as Canada, England, or Nigeria?
- Have you been asked to PAY money to receive a deposit from another country such as Canada, England, or Nigeria?
- Are you receiving PAY or a COMMISSION for facilitating money transfers through your account?
- Did you respond to an email requesting you to CONFIRM, UPDATE, OR PROVIDE your account information?

TELL BRANCH PERSONNEL IMMEDIATELY!

DON'T GET RIPPED OFF!

ADDITIONAL RESOURCES

The state of 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/elder.shtml>

Can Bank Tellers Tell? – Legal Issues Relating to Banks Reporting Financial Abuse of the Elderly.
American Bar Association 2003 Publication available at

http://www.abanet.org/aging/bank_reporting.pdf

TRIAD Handbook – designed to assist law enforcement and senior citizens in implementing a comprehensive crime prevention program for older adults

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

BITS' RECOMMENDATIONS FOR WHAT CONSUMERS SHOULD KNOW AND CAN DO TO PROTECT THEMSELVES

What Consumers Should Know

- Hundreds of millions of financial transactions—both online and offline—occur each day.
- On the whole, Internet banking and other online financial transactions are safer than paper-based transactions.
- Identity thefts that occur online are generally smaller and take less time to resolve than paper-based thefts.
- Identity theft is a highly complex issue with many players and no simple solutions.
- Incidents of identity theft and identity fraud are often mis-characterized in the popular media.
- Fraudulent credit and debit card transactions are not identity theft and seldom lead to identity theft.
- Most cases of identity theft do not occur online. Where the method is known, most theft of personal information is through traditional rather than electronic channels—68.2% obtained offline versus 11.6% obtained online. (Source: 2005 Identity Fraud Survey Report by Javelin Strategy and Research)
- Resolving identity theft requires coordination among multiple federal, state and local agencies, and industry.
- Consumers are protected against financial losses from fraud by laws and regulations.
- Customers will be held harmless in almost all circumstances in which fraud occurs and is reported to their financial institution timely and accurately.
- Financial institutions use sophisticated systems to flag unusual activity and protect consumers against fraud. These systems allow financial institutions to monitor activities in real time.
- Many of these controls are kept “invisible” for security reasons.

What Consumers Can Do

- **Know what you are signing.** Ensure you understand the documents you are signing and the authority you may be granting.

- **Never allow unsolicited contractors into your home.** Check with the Better Business Bureau or obtain references from trusted family and friends before hiring contractors to perform services.
- **Never give money to a stranger.** Regardless of what is promised as a reward, such as in cases of found valuables or cash, you should never provide cash to people you do not know. Never send money to win or inherit money. Legitimate lotteries do not require up-front payment. Consult your attorney if contacted regarding an inheritance.
- **Be careful of requests by phone.** Scammers can use the telephone as a means to reach victims. Be careful of charitable requests and solicitations. The phone company will never call you and ask you to call them back to conduct a test. The series of numbers the scammer asks you to dial may allow him/her to make long distance phone calls and bill them to you.
- **Know your merchant.** Ensure you know the person or entity to which you are giving information over the Internet, phone, or fax. Do not provide your personal information unless you have initiated contact with the merchant. Only do business with Internet companies that use a secure form, often indicated by a padlock in the lower corner of the website, to capture private information such as account numbers or credit card numbers.

Order copies of your credit report at least once a year from each of the three major credit bureaus and ensure all of the information is accurate. Stagger the process so you can check your records three times each year. You are entitled to receive one free credit file disclosure every 12 months from each of the nationwide consumer credit reporting companies – Equifax, Experian and TransUnion. This free credit file can be requested through the following websites and phone numbers:

Equifax www.equifax.com 1-800-685-1111

Experian www.experian.com 1-888-EXPERIAN (397-3742)

Transunion www.transunion.com 1-800-916-8800

- **Monitor your accounts and statements frequently and thoroughly,** ensuring that all activity is accurate. If your account statements are late, immediately contact your financial institution(s) to ascertain if and when the statements were mailed. If your institution offers online banking, check your account frequently and regularly, rather than waiting for monthly statements. Reporting fraud as soon as possible helps stop further occurrences of fraud.
- **Always thoroughly tear or shred documents with personal information,** such as pre-approved credit offers, **unused instant credit offers** which may contain account information, Social Security numbers, date of birth, etc. Shredding such documents protects you against “dumpster diving.”

- **Always protect your account information.** Don't write your personal identification number (PIN) on your ATM or debit card. Don't write your Social Security number and/or credit card number on a check. Never give out your account numbers or social security numbers to someone claiming to be from your financial institution.
- **Safeguard your checkbook, receipts, identification card or driver's license information, account numbers and account expiration dates.** Don't leave your checks or credit card records, including your transaction receipts, or anything else with credit card numbers and expiration dates in unsafe locations.
- **When using your ATM, cover your hand when entering the PIN number** to protect the information from "shoulder surfers."
- **Carry only those pieces of identification you absolutely need,** and keep them secure.
- **Check merchant privacy policies** and only shop at those that publish privacy policies with which you agree.
- **If you suspect your identity has been stolen or you have shared any personal financial data, including your account username and password, contact your financial institution and the authorities immediately.** U.S. consumers should:
 - File a police report with their local police department and call the Federal Trade Commission at 1-877-ID-Theft, or www.ftc.gov.
 - Complaints can also be reported to: the Internet Fraud Complaint Center (IFCC), www.ifccfbi.gov.
 - Contact the three credit reporting agencies to place a fraud alert on your record. Contact information can be found [above](#).
 - Maintain a log of all contacts you make with the authorities regarding the matter, including the name, title, phone number and police case number, in case future contact is required.
- **Watch your wallet.** The most frequently reported source of information used to commit fraud was a lost or stolen wallet or checkbook; computer crimes accounted for just 11.6 percent of all known-cause identity fraud in 2004 – and half these digitally-driven crimes stem from spyware, software the computer user unknowingly installs to make ads pop-up when the consumer is online. The use of anti-virus, anti-spam or anti-spyware software may help to prevent such fraud.
- **Be careful who you trust.** Among cases where the perpetrator's identity is known, half of all identity fraud is committed by a friend, family member, relative, neighbor or in-home employee – someone known by the victim.
- **Keep your eyes open.** The majority of actual identity fraud crimes in the United States are self-detected. This reinforces the benefits of activity monitoring through electronic review of transactions, statements and credit reports allowing consumers to check their account activities quickly and efficiently – without waiting for a paper bill or statement.

Victims of identity theft who detected the crime by monitoring accounts online experienced financial losses that were less than one-eighth of those who detected the crime via paper statements.

- **If you do business on the Internet:**
 - Use firewalls and anti-virus software to detect messages with malicious payloads, or hackers attempting to take control of your computer
 - Bookmark all of your financial services web sites and only access them using your “Favorites” menu
 - Never click on a hyperlink provided in a e-mail
 - Consult with a computer expert for advice on the best technology available
 - Delete unsolicited or unknown e-mails
 - Report suspicious e-mails to your financial institution
 - Be diligent – Don’t respond to any request for personal information and monitor your accounts regularly