

BITS

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

BITS FRAUD PROTECTION GUIDE: PROTECTING THE ELDERLY AND VULNERABLE FROM FINANCIAL FRAUD AND EXPLOITATION

SEPTEMBER 2005

**A PUBLICATION OF THE
BITS FRAUD REDUCTION STEERING COMMITTEE**

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

BACKGROUND

Reports of financial exploitation and other forms of abuse, particularly among the elderly and vulnerable, is an increasing problem and concern to society. This paper has been developed as an educational tool to assist in raising awareness of the problem, and how to prevent or mitigate it.

The National Research Council estimates between 1 and 2 million Americans age 65 or older have been injured, exploited, or otherwise mistreated by someone on whom they depended for care or protection.* The 1998 National Elder Abuse Incidence Study found that Adult Protective Services (APS) agencies substantiate more cases of financial abuse than physical abuse each year and that only one in five cases of abuse, neglect and exploitation is reported to authorities.

The 2001 study by the National Association of Adult Protective Service Administrators (NAAPSA) reported 38,015 documented reports of financial exploitation of the elderly and vulnerable. The study also states that only 1 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 an elderly 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 and is often traced to family members, trusted friends, or caregivers. Financial abuse often occurs with the implied acknowledgment and consent of the elder person and can be more difficult to detect.

The financial services industry is often the first to detect a change in the pattern of customers with whom they have regular contact. This puts institutions in a unique position to assist in protecting customers and upholding the inherent trust relationship with clients. Misconceptions and misunderstandings of privacy laws often cause an institution to not report incidences even though many state laws mandate reporting. The National Adult Protective Services Association (NAPSA) July 2003 survey found that banks 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), which 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 customers for potential abuse, however, it is an area in which financial institutions may make a positive contribution to the well-being of customers who may be vulnerable to such abuse.

TYPES OF ABUSE

NCEA recognizes seven types of elder abuse. In addition to signs of financial abuse, financial center personnel may recognize, identify and report other forms of abuse. Forms of abuse other than

* “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>)

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

financial abuse may be indicators that financial abuse is also occurring. The types of abuse below may or may not be independent of each other.

- **Self neglect** – Failure by oneself to provide goods or services essential to avoid a 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).
- **Active neglect** – Intentional failure to fulfill care-giving obligations, infliction of physical or emotional stress or injury, abandonment, denial of food, medication, personal hygiene, etc.
- **Physical abuse** – Infliction of physical pain or injury, etc.
- **Sexual abuse** – Non-consensual sexual contact of any kind with an elderly person.
- **Abandonment** – Desertion of an elderly person 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** – Illegally or unethically exploiting by using funds, property, or other assets of an older person for personal gain.

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

- **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 Power of Attorney, real estate transaction, 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. Scams against the vulnerable and elderly, which also affect the public at large, include but are not limited to:

- **Advance fee fraud or “419” fraud** – Named after the relevant section of the Nigerian Criminal Code, this fraud is a popular crime with the West African organized criminal networks. There are a myriad of schemes and scams—mail, email, fax and telephone promises designed to facilitate victims’ parting with money. All involve requests to help move large sums of money with the promise of a substantial share of the cash in return.
- **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 con artists.
- **Bank employee/examiner fraud** – The victim believes that he or she is assisting authorities in gaining evidence that will lead to the apprehension of a bank employee or examiner that is committing a crime. The victim is asked to provide cash to bait the crooked employee.
- **Bank employee fraud** – The perpetrator calls the victim pretending to be a security officer from the victim’s bank advising 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.
- **Itinerant fraud** – Victims are intimidated into paying unreasonable amounts for poor quality work, i.e., door-to-door solicitations for roofing or paving, auto body repair scams, etc. Often the work is fully paid for, but only partially completed.

- **International lottery fraud** – Scam operators, often based in Canada, are using the telephone and direct mail to notify the victim that he or she has won a lottery and an advance check is included. Victim is then 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.
- **Relative in distress** – The perpetrator calls the victim pretending to be a relative in distress and in need of cash and asks that money be transferred into a bank account.
- **Misappropriation of income or assets** – A perpetrator, often a family member or caregiver, obtains access to an elder'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** – A perpetrator uses 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) and uses or attempts to use that information to establish or take over a credit, deposit, or other financial account (“account”) in that person’s name.
- **Telemarketing scams** – A perpetrator persuades a victim to buy a valueless or nonexistent product, donate to a bogus charity or invest in a fictitious enterprise.
- **Fake prizes** – A perpetrator claims the victim has won a nonexistent prize or lottery 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.
- **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.

RED FLAG INDICATORS OF FINANCIAL EXPLOITATION

Signs of financial or material exploitation include but are not limited to:

- Sudden changes in bank account or banking practice, including an unexplained withdrawal of large sums of money by the elder who is escorted by another (e.g. caregiver, family member, “friend”, etc.);
- The recent addition of authorized signers on an elder's bank signature card;
- Unauthorized withdrawal of the elder's funds using the elder's ATM card, particularly repetitive withdrawals over a short period inconsistent with prior usage patterns;
- 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 availability of adequate financial resources;
- Discovery of an elder's signature being forged for financial transactions or for the titles of his/her possessions;
- Sudden appearance of previously uninvolved relatives claiming their rights to an elder's affairs and possessions;
- Elder has companion who seems to be “calling the shots;”
- Elder has no knowledge of newly issued ATM or debit card on account;
- Elder is confused about the account balance or transactions on their account;
- A caregiver is getting paid too much or too often;
- Request for a new power of attorney that the elder does not appear to understand;
- Elder reports concerns about giving out personal and account information to a solicitor via the phone or email;

- Unexplained sudden transfer of assets to a family member or someone outside the family;
- Excitement about winning a sweepstakes or lottery;
- Provision of services that are not necessary;
- An elder's report of financial exploitation²; and
- Sudden appearance of credit card balances with no prior history of using credit.

ADDRESSING LIABILITY CONCERNS

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 banks. 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.

INSTITUTING A PREVENTION PROGRAM

To protect assets and reduce fraud against vulnerable customers and to generate goodwill within communities, financial institutions should institute a prevention program to raise awareness and educate staff to identify, prevent, and report suspected cases of financial exploitation. Roles of various departments include:

- Branch Office
 - Identify the situation – Recognize warning signs through changes in the customer’s activity or behavior.
 - Avoid confrontation – Try to separate the client from the suspect.
 - Determine consumer intent – Use probing questions but let the customer tell you in his or her own words without prompting.
 - Delay the suspicious transaction, if possible.
 - Contact loss management/fraud department.
 - Be aware of recent or new scams and fraud schemes.
- Loss Management/Fraud Department
 - Document the situation.
 - Take immediate proactive action on accounts through normal prevention and recovery steps.
 - Send telephone report to Adult Protective Services.*
 - Provide necessary research and investigative assistance to APS, as needed.
 - Monitor account during legal proceedings.
 - Advise financial center branch office of final outcome.

APS programs are charged with taking reports, doing investigations and providing services to vulnerable adults who have physical or mental disabilities that prevent them from protecting themselves from abuse, exploitation and neglect by themselves or others. There is no federal APS statute. APS programs are governed by state laws that vary from state to state. Reports to APS are confidential. Upon receipt of a report, APS will contact the customer and affiliated parties, investigate and review the situation, contact law enforcement, if necessary, make a determination and report back to the financial institution.* To obtain the APS reporting number in your area, contact the Eldercare Locator at 1-800-677-1116 or www.eldercare.gov.

² The National Center on Elder Abuse (<http://www.elderabusecenter.org/default.cfm?p=basics.cfm>)

NEXT STEPS

The BITS Fraud Reduction Steering Committee will conduct a short-term project to examine strategies for implementing or improving a financial institution internal prevention program for education and awareness. This project, which will be led by Linda Mill, Senior Vice President, Loss Management Department, Wachovia Corporation, will develop a toolkit for educating financial center and loss management personnel. An invitation to participate in this project will be sent to the BITS membership and institutions are encouraged to participate. For more information, please contact Robin Slade, Senior Consultant, BITS, at 630-653-9340 or at rmslade@sbcglobal.net.

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 Trends
- Identity Theft
- Internet Fraud
- Legal and Regulatory
- Loan Fraud
- Shared Databases

This paper was created with the assistance and expertise of Linda Mill, Senior Vice President, Wachovia, and 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, a nonprofit consortium of 100 of the largest financial institutions in the US, was created in 1996 to foster the growth of electronic commerce for the benefit of financial institutions and their customers. Throughout its work, 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. The BITS Committee within the Board of Directors of The Financial Services Roundtable is composed of the chairmen and CEOs of some of the largest U.S. financial services holding companies.

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