November 30, 2015

Via pubcom@finra.org

Marcia E. Asquith
Office of the Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 20006-1506

Re: Regulatory Notice 15-37—Financial Exploitation of Seniors and Other Vulnerable Adults

Dear Ms. Asquith:

The Financial Services Roundtable ("FSR")[1] appreciates the opportunity to comment on FINRA's proposed (i) amendments to its current Rule 4512 (Customer Account Information) and (ii) new Rule 2165 (Financial Exploitation of Specified Adults) (jointly, the "Proposals").[2] The proposed amendments to Rule 4512 would require FINRA members ("firms") to make reasonable efforts to obtain the name of and contact information for a "trusted contact person" for each retail customer's account.

---

1 As *advocates for a strong financial future*™, FSR represents the largest integrated financial services companies providing banking, insurance, payment, 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. FSR member companies provide fuel for America's economic engine, accounting directly for $92.7 trillion in managed assets, $1.2 trillion in revenue, and 2.3 million jobs.

2 Regulatory Notice 15-37, Financial Exploitation of Seniors and Other Vulnerable Adults (October 2015), *available at* http://www.finra.org/sites/default/files/notice_doc_file_ref/Regulatory-Notice-15-37.pdf.

Proposed Rule 2165 would permit (but not require) a "Qualified Person" of a firm to place temporary holds on disbursements of funds or securities from the "Account" of a "Specified Adult" if there is a reasonable belief of "financial exploitation" of the customer.

I. Executive Summary

- FSR supports a uniform and coordinated approach to protect senior investors and vulnerable adult investors.
- FSR urges FINRA to coordinate with other regulators to address the Proposals' significant potential legal risks to firms.
- FSR urges FINRA to adopt a principles-based rule that would permit a firm to develop compliance tools in keeping with its unique business model.
- Expanding Rule 2165 beyond "disbursements" to include "transactions" would provide significantly more robust protections for seniors and vulnerable adults.
- FSR urges FINRA to provide guidance regarding who can be designated as a trusted contact person, and require the trusted contact person's acknowledgment of this designation.
- Proposed Rule 2165 should address the information that firms can share with the trusted contact person, and with other financial services firms.
- FINRA should expressly allow firms to use the Temporary Hold period(s) to seek intervention by the relevant governmental agencies.
- FSR urges FINRA to clarify the scope of the internal review requirement.
- Proposed record retention provision would impose new books and records requirements, which will result in substantial actual costs to firms in addition to potential legal risks.
- FINRA's Economic Impact Assessment fails to demonstrate that the designation of a trusted contact person would be an effective mitigant against financial exploitation of the elderly and vulnerable adults. FSR urges FINRA to present findings that show evidence that a customer designating a trusted contact person is, or is likely to be, an effective mitigant against the financial abuse that the Proposals are intended to address.

II. Introduction

FSR has long supported efforts to protect senior investors, as demonstrated, in part, by its many efforts to educate older Americans ("senior investors") as they prepare for retirement.[3] BITS (FSR's technology policy division)[4] has been at the forefront of initiatives to protect senior investors and provide fraud-reduction resources to the financial services industry.[5]

FSR applauds FINRA for the steps that it, too, has taken to educate senior investors and to provide resources to these investors, including through its Senior Helpline. The reports that FINRA, the United States Securities and Exchange Commission ("Commission"), and the North American Securities Administrators Association ("NASAA") have published over the past eight years are useful resources for the financial services industry in developing practices, policies, and procedures related to senior investors.[6]

---

3 A sampling of FSR's financial education efforts with respect to senior investors can be found at http://fsroundtable.org/financial-literacy/.

4 BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services.

5 *See* BITS AND THE FINANCIAL SERVICES ROUNDTABLE, *Elder Financial Exploitation Prevention*, 2015 (Webinar advocating awareness on issues related to elder financial abuse such as emerging elder fraud scams, industry efforts to combat abuse and provide resources for the financial services community (2015); Roxane Schneider, *FSR Members Thwart Fraud Perpetrators* (BITS and The Financial Services Roundtable), 2014, *available at* http://fsroundtable.org/bits/world-elder-abuse-awareness-day/; BITS AND THE FINANCIAL SERVICES ROUNDTABLE, *BITS At-Risk Adult Training Curriculum*, 2013, *available at* http://www.bits.org/publications/doc/BITS-RoundtableAt-RiskAdultTrainingCurriculumJan2013.pdf; BITS AND THE FINANCIAL SERVICES ROUNDTABLE, Statement of BITS President Paul Smocer On Behalf Of The Financial Services Roundtable Before The Special Committee On Aging Of The U.S. Senate, *America's Invisible Epidemic: Preventing Financial Elder Abuse*, Nov. 15, 2012, *available at* http://www.bits.org/publications/regulation/BITSTestimonySenateAging15Nov12.pdf; BITS AND THE FINANCIAL SERVICES ROUNDTABLE, *FSR Older Americans Financial Abuse Prevention Working Group*, June 2012), *available at* http://www.bits.org/publications/doc/RoundtableWEAADBookletJune2012.pdf; BITS AND THE FINANCIAL SERVICES ROUNDTABLE, *Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation*, April 2010, *available at* http://www.bits.org/publications/fraud/BITSProtectingVulnerableAdults0410.pdf.

6 *See, e.g.*, SEC. & EXCH. COMM'N, Office of Compliance Inspections and Examinations and FINRA, *National Senior Investor Initiative—A Coordinated Series of Examinations* (Apr. 15, 2015), *available at* https://www.finra.org/sites/default/files/SEC%20National%20Senior%20Investor%20Initiative.pdf; SEC. & EXCH. COMM'N, Office of Compliance Inspections and Examination, NASAA, and FINRA, *Protecting Senior Investors: Compliance, Supervisory and Other Practices Used by Financial Services Firms in Serving Senior Investors* (Sept. 22, 2008), *available at* http://www.sec.gov/spotlight/seniors/seniorspracticesreport092208.pdf; and SEC. & EXCH. COMM'N, Office of Compliance Inspections and Examination, NASAA, and FINRA, *Protecting Senior Investors: Report of Examinations of Securities Firms Providing "Free Lunch" Sales Seminars* (September 2007), *available at* https://www.finra.org/sites/default/files/Industry/p036814.pdf.

III. FSR supports a uniform and coordinated approach to protect senior investors and vulnerable adult investors

FINRA noted in Regulatory Notice 15-37 that proposed Rule 2165 could create potential liability for firms and their associated persons. FINRA's discussion centers on a firm's determination to disburse or withhold funds; but FINRA provides no analysis of potential conflicts with broker-dealers' obligations under state or federal law with respect to privacy or other consumer protection requirements. Further, there is no indication that FINRA has consulted with state or federal authorities regarding the interplay of the Proposals with consumer protection requirements, including with respect to privacy.

Before finalizing the Proposals, FSR believes that FINRA should confer with the states (represented by NASAA) as well as the Commission in order to reconcile the Proposals with firms' existing legal and regulatory requirements and to eliminate potential conflicts among those requirements. The outcome of such discussions should be published by FINRA for firms and investors to consider and reflect in their respective comments regarding the Proposals. FSR further believes that the end result should be national standards to achieve a uniform and coordinated approach to this important component of investor protection, rather than the *ad hoc* approaches that will be the outcome if FINRA, through the Proposals, and each of the states pursue separate initiatives.[7]

IV. FSR urges FINRA to coordinate with other regulators to address the Proposals' significant potential legal risks to firms

Notwithstanding the collaboration of FINRA, the Commission, and NASAA on other senior investor initiatives, the Proposals do not appear to reflect input from any other federal or state governmental agency or regulatory organization. In light of the potential for civil—and possibly criminal—liability risks that the Proposals may create for firms and their associated persons, the absence of coordination with relevant authorities and companion rulemaking raises substantial concerns. FINRA itself notes that " . . . there may be significant impacts with respect to legal risks and attendant costs to firms that choose to rely on the proposed rule in placing temporary holds on disbursements; although the direction of the impact is ambiguous."[8]

If adopted as proposed without corollary action by the states or the federal government, firms and their associated persons will be faced with the dilemma of: (i) refraining from

---

[7] FINRA noted that Delaware, Missouri, and Washington State have each enacted legislation permitting broker-dealers and other financial institutions to place temporary holds on disbursements and transactions if they suspect financial exploitation of specified persons. *See* Regulatory Notice 15-37, *supra* note 2, at page 9, endnote 4 *citing* Del. Code Ann. tit. 31, § 3910 (2015); Mo. Rev. Stat. §§ 409.600-.630 (2015); and Wash. Rev. Code §§ 74.34.215, 220 (2015).

[8] *See* Regulatory Notice 15-37, *supra* note 2, at 6.

disbursing funds or securities, which potentially could result in economic hardship to customers (*e.g.*, if the funds were needed to pay medical expenses or to satisfy other financial obligations, such as mortgage payments); or (ii) disbursing funds and securities based either on Supplementary Material .01 to Rule 2165, which states that "[t]his Rule does not require members to place temporary holds on disbursements of funds or securities from the Account of a Senior Adult, or because, based on the limited information available to it, the firm determined that it did not have a reasonable basis to believe that the customer was the subject of financial exploitation."

We, note, however that many situations do not involve a *reasonable basis of belief*. For example, some situations start out with a red flag or suspicion of possible wrong-doing that creates a duty to investigate to avoid liability. As such, FSR believes a "reasonable basis to suspect the customer may be the subject of financial exploitation" may be a better standard.

Although FINRA proposes to provide a safe harbor when firms exercise discretion in placing temporary holds on disbursements of funds or securities under the circumstances specified in proposed Rule 2165,[9] the scope of the safe harbor may in practice provide only limited protection to firms. Moreover, if proposed Rule 2165 is adopted without companion federal and state action, a "Catch-22" situation would be created because the mere existence of Rule 2165 may create liability for firms that do not withhold disbursements, even though the supplementary language expressly provides that Rule 2165 does not create any obligation.

Accordingly, FSR urges FINRA to engage with federal and state regulators to address in a comprehensive manner the potential significant legal risks the Proposals pose for firms that could arise as a result of multiple and conflicting legal or regulatory requirements imposed by governmental authorities and FINRA.

V. FSR urges FINRA to adopt a principles-based rule that would permit a firm to develop compliance tools in keeping with its unique business model

FINRA solicited comment on whether it should "mandate specific procedures for escalating matters related to financial exploitation."[10] FSR believes that firms that intend to rely on the proposed safe harbor provided by Rule 2165 should be allowed to develop their own policies and procedures reasonably designed to achieve compliance with the conditions of the safe harbor, (including determining their own internal escalation procedures), which would be based on each firm's business model. Accordingly, FSR recommends that FINRA replace the prescriptive approach in proposed Rule 2165 with a principles-based approach that would allow

---

9 *See* proposed Supplementary Material .01 to Rule 2165.

10 *See* Regulatory Notice 15-37, *supra* note 2, at 8 (Question 11).

a firm to develop policies and procedures within its supervisory system[11] based upon its unique business model, rather than a "one-size-fits-all" prescriptive rule.

FSR also recommends changes to the definition of "Qualified Person."[12] First, FSR believes that the definition of "Qualified Person" should be revised to eliminate the provision that a person acting in a legal or compliance capacity is qualified *per se*. Legal and compliance personnel seldom witness the events that give rise to a suspicion of exploitation (transactions, personal interaction, *etc*.). As a result, while legal and compliance departments will likely advise and guide customer-facing personnel when these situations arise, legal and compliance personnel are rarely, if ever, in a position to substitute their judgment for the judgment of customer-facing personnel.

Additionally, in our view, the phrase "reasonably related to the account," used to describe those personnel of the firm that are authorized to place a hold, ought to be eliminated or clarified. Firms ought to be allowed, in their discretion, to establish the processes for detecting and addressing suspected exploitation that best fit their customer base and risk profile. Indeed, many firms have done so, for purposes of compliance with state laws requiring them to report suspected or detected elder abuse. It is highly likely that the service areas supporting these processes do not have relationships to particular Accounts. Therefore, the inclusion of the "reasonably related" phrase will at a minimum require firms to assess current processes to ensure that persons placing a hold on the Account are "reasonably related to the account." It might require firms to incur financial and operational costs to review and possibly revamp existing infrastructure that is already working satisfactorily in order to achieve technical compliance with the rule. We believe that "Qualified Person" is a designation that firms should confer on those groups or individuals best positioned to administer the firm's programs addressing exploitation.

VI. Expanding Rule 2165 to include "transactions" would provide significantly more robust protections for seniors and vulnerable adults

FINRA should expand the rule beyond "disbursements" and include "transactions." The focus solely on "disbursements" unnecessarily limits the protections provided by proposed Rule 2165. The inclusion of "transactions" (as permitted in the Delaware law) would provide significantly more robust protections for seniors and vulnerable adults. For example, under the current language in proposed rules, should an exploitative liquidation of investments occur, the firm would only be protected by the proposed safe harbor afforded by proposed Rule 2165 when if refuses to disburse the fruits of the exploitative sale, but would receive no protections for

---

11 *See* FINRA Rule 3110.

12 As proposed, a "Qualified Person" means "an associated person of a member who serves in a supervisory, compliance or legal capacity that is reasonably related to the Account of the Specified Adult." *See* paragraph (a)(3) of proposed Rule 2165.

refusing the initial sale of the investment—an action that can be almost as damaging to an investor as the disbursement.

We note that transactions also can trigger significant tax consequences (*e.g.*, a liquidation of securities or an IRA); incur fees or cause other negative financial implications for the senior or vulnerable investor because the transaction may not be suitable or may be inconsistent with a client's risk tolerance; or expose the senior or vulnerable investor to financial losses. Other examples of exploitative, non-disbursement transactions include: the buying of an investment product for the benefit of the wrong-doer, a change in ownership of an Account, a change in the beneficiary of an Account, or incurring penalties due to another change in the Account (such as annuity-related surrender charges).

VII. FSR urges FINRA to provide guidance regarding who can be designated as a "trusted contact person," and require the trusted contact person's acknowledgement of this designation

Proposed new paragraph (a)(1)(F) of Rule 4512 would require that a firm make reasonable efforts to obtain the name of and contact information for a "trusted contact person" who may be contacted about an Account. The Proposals do not clarify what activities constitute "reasonable efforts" by a firm to obtain the identity of a trusted contact person. For currently existing account owners, would this include a disclosure or questionnaire in what the industry refers to as the "SECBAR letter" that is mailed to clients at least once every three (3) years? For new accounts, would this question be asked in the new account documents? Moreover, the only qualifications for a trusted contact person are that he or she be at least 18 years of age, and not be authorized to transact business on behalf of the account. There is no requirement that the trusted contact person be an immediate family member, or have any professional training in determining the mental state of the customer or the appropriateness of any disbursement from or other activity in the Account.

In general, we believe the customer should have discretion to designate any adult as a "trusted contact person" for the Account (including persons to whom the customer granted a power of attorney with respect to the Account), and that the firm should have the benefit of the safe harbor contemplated in proposed Rule 2165 for acting in accordance with the customer's designation. FSR recommends that FINRA require that the "trusted contact person" acknowledge his role at the time of designation (or at Account opening, for a new account), because the "trusted contact person" may take on legal liability due to his actions or inactions. We also believe it would be helpful for the final rule to provide that firms may obtain contact information for a successor/alternate "trusted contact person." However, due to liability concerns, registered representatives should be prohibited from being designated as a "trusted contact person."

The Proposals only require firms to seek information regarding trusted contact persons at the time of Account opening and when a firm updates account information as part of its regular process pursuant to rule 17a-3 under the Securities Exchange Act of 1934[13] or as otherwise required by applicable law or rule. FSR asks FINRA to clarify that if a customer does not direct a firm to remove or replace the trusted contact person, the firm is not liable if it contacts the trusted contact person previously designated by the customer as reflected in the firm's books and records. As discussed above, FSR believes that FINRA should coordinate with appropriate federal and state authorities to ensure that firms will not have legal liability for contacting trusted contact persons or immediate family members pursuant to the Proposals.

FSR further notes that proposed Rule 2165 does not specify the role of a trusted contact person and the extent to which a firm should or is required to rely on information provided by the trusted contact person. FSR is concerned that firm interactions with trusted contact persons could place a firm and its associated persons in the role of mediating disagreements among a customer, the trusted contact person, and the proposed payee with respect to disbursals from an Account. Furthermore, a firm could even be placed in the precarious position of mediating family disputes if it were to contact an immediate family member in lieu of a trusted contact person in accordance with paragraph (b)(1)(B)(ii) of proposed Rule 4512. In many circumstances, there will be conflicting information and firms will not be able to determine the appropriate course of action to take. Actions taken and decisions made under these complex—and often emotional—circumstances should not be the responsibility of firms.

In the absence of a trusted contact person, or if a trusted contact person is suspected of being involved in the financial exploitation, FINRA proposes to permit firms to discuss possible exploitation with immediate family members. FSR further believes that firms should be permitted to contact and discuss matters with the customer's accountants and/or attorneys if the customer has authorized these communications. FSR urges FINRA to clarify that where "time is of essence," the firm may in its discretion contact an immediate family member in instances in which the trusted contact person is not immediately available.

FSR believes that such modifications to the Proposals would help mitigate potential issues regarding inconsistencies with a customer's indicated preference, such as when a customer has authorized a firm to share Account information with an attorney or accountant, or has appointed a power of attorney to an Account. Among other things, these modifications, if adopted, would preserve the customer protections of permitting a firm to contact an immediate family member if it has a reasonable basis to suspect that the trusted contact person is, was, or will be involved in financial exploitation of the customer.

---

[13] 17 C.F.R. § 240.17a-3.

VIII. Proposed Rule 2165 should address the information that firms can share with the trusted contact person, and with other financial services firms

As proposed, Rule 2165 does not address the scope of information that can be shared with the Account's trusted contact person. In September 2013, eight federal agencies jointly issued guidance to clarify that "reporting suspected financial abuse of older adults to appropriate local, state, or federal agencies does not, in general, violate the privacy provisions of the [Gramm-Leach-Bliley Act] or its implementing regulations."[14] As a consequence, firms are uncertain as to what additional information they can share with a governmental agency (even in mandatory reporting states) beyond the information the firm is required to include in the initial report. This uncertainty will only increase with respect to third parties who are not authorized to act on an Account, as will be the case with the "trusted contact person." FSR urges FINRA to provide the necessary guidance to aid firms in handling information under the circumstances presented in these very difficult situations. We believe the firm also should be permitted to share information with a contra-broker-dealer in the event the Account is in the process of transferring out. Uncertainty about what information firms can share (and with whom) will compromise the effectiveness of any final rule adopted under the Proposals.

FINRA should expressly permit holds on ACATS transfers, and should permit firms to share information concerning the Account with financial institutions which are receiving counterparties of an Account transfer. FSR members have observed that an individual who seeks to gain control or exploit a senior or vulnerable adult will submit an ACATS request in order to avoid an advisor with whom the customer has a familiar and trusted relationship and move the customer's assets to an institution that is unfamiliar with the customer.

IX. FINRA should expressly allow firms to use the Temporary Hold period(s) to seek intervention by the relevant governmental agencies

Proposed Rule 2165 provides for a temporary hold of up to 15 business days on Account assets, which may be extended one time for another 15 business days. However, proposed Rule 2165 does not specify the steps that firms should take with respect to Account assets at the expiration of Rule 2165 hold(s) if there remains a reasonable belief of financial exploitation with respect to the relevant Specified Adult. As proposed, FSR is concerned that Rule 2165 would require firms would to release assets notwithstanding a reasonable suspicion, or even a determination, that financial exploitation has, did, or will occur.

---

[14] *See* "Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults," *available at* http://www.federalreserve.gov/newsevents/press/bcreg/bcreg20130924a2.pdf. The guidance was issued by the following agencies: Board of Governors of the Federal Reserve System, Commodity Futures Trading, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency, and Securities and Exchange Commission.

To protect against such an outcome, which clearly would be inconsistent with the stated purpose of the Proposals, FSR recommends that any final rule permit firms to impose a temporary hold on an Account for up any period within the reasonable discretion of the firm, or until a third party notifies the firm that the need for the hold has expired (*e.g.*, action by adult protective services, or an order of a court of competent jurisdiction), or subsequent events show that the threat no longer exists. FSR further recommends that any final rule permit firms to petition a governmental agency for a determination concerning the proposed disbursement, which would allow the applicable jurisdiction's adult protective services to intervene.

In addition, if the customer has a durable power of attorney, the individual granted that authority could be designated as a trusted contact person to discuss possible concerns with a proposed disbursement, which would allow this individual to direct a temporary hold on Account assets in order to provide the individual the opportunity to obtain a court order freezing the Account.

Finally, FINRA proposes to require that firms provide notice that they have imposed a temporary hold no later than two (2) business days following the imposition of a temporary hold on the Account. Due to the complexity of the proposed notification requirements, FSR recommends that proposed Rule 2165(b)(1)(B) be revised to require a firm to provide notice of a temporary hold no later than five (5) business days after it was imposed, and to clarify when the time period commences and terminates. For example, if a firm decides to place a temporary hold on May 1st at 2:15 p.m. (PT), does the firm have until 2:15 p.m. (PT) on May 3rd to take action? Until the close of business on May 3rd? Also, what form of notice would be acceptable? Would leaving a voice message or e-mail be acceptable? If notifying by regular U.S. MAIL, what is deemed within the two (2) business days' requirement—placing the notice into the mail, or must the notice be delivered to the customer within the required number of business days? FRS requests clarification so that firms can comply with applicable deadlines.

X. FSR urges FINRA to clarify the scope of the internal review requirement

Pursuant to paragraph (b)(1)(C) of proposed Rule 2165, once a firm places a temporary hold on disbursements from an Account, it must initiate an internal review of the facts and circumstances causing a Qualified Person to have a reasonable belief that there has, was, or will be financial exploitation of the Specified Adult. We note that firms will not have access to relevant information, including: (i) the Specified Adult's medical professionals; (ii) detailed or complete information about the proposed disbursement; and/or (iii) the identity of immediate family members or other close relatives. Further, in some cases, firms will not necessarily have the necessary expertise or complete information to allow them to evaluate the appropriateness of Account disbursements. FSR respectfully requests that FINRA clarify the scope of the internal review requirement, including the factors to be considered and the nature of inquiry that firms must conduct.

XI. Proposed record retention provision would impose new books and records requirements, which will result in substantial actual costs to firms in addition to potential legal risks

Although the Proposals would impose substantial new books and records requirements on firms, FINRA did not address the economic impact of such requirements in its Economic Impact Assessment. FSR believes the Proposals, particularly those related to obtaining and updating additional information with respect to customer accounts, making determinations of financial exploitation, documenting such determinations, and conducting and documenting internal reviews would require firms to devote substantial work on systems and processes to build these new requirements into the firm's verification process. If adopted as proposed, we believe the Proposals will result in substantial actual costs for firms in addition to the potential legal risks discussed above. FSR urges FINRA to address the economic impact of the proposed books and records requirements.

XII. FINRA's Economic Impact Assessment fails to demonstrate that the designation of a trusted contact person would be an effective mitigant against financial exploitation of the elderly and vulnerable adults

Unfortunately, the predominate source of financial exploitation of the elderly and other vulnerable adults reportedly is the person's family, which by some estimates represent almost 75 percent of this criminal activity.[15] However, FINRA's Economic Impact Assessment fails to examine the potential efficacy of the Proposals with a view to assessing the most likely source of financial exploitation of the elderly and vulnerable adults. FSR urges FINRA to present findings that show evidence that a customer designating a trusted contact person is, or is likely to be, an effective mitigant against the financial abuse that the Proposals are intended to address.

FSR believes it is important for FINRA to determine how well the Proposals will work, and how effective the Proposals will be *vis-à-vis* reporting to the applicable jurisdiction's adult protective service (under mandatory or permissive reporting statutes) or other potential mitigants. Absent further analyses, FSR is concerned that the Proposals would impose substantial risks to firms without evidence of a corresponding benefit to anyone.

****

[15] *See*, Paul Smocer, STATEMENT FOR THE RECORD BEFORE THE SPECIAL COMMITTEE ON AGING OF THE U.S. SENATE at 1 (Nov. 15, 2012) (stating that "the most frequent perpetrators of financial abuse are family members, who by some estimates commit nearly 75% of crimes"); BITS, "Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation" at 4 (Apr. 2010) (noting that "exploitation is often traced to family members, trusted friends, or caregivers").

FSR appreciates the opportunity to comment on Regulatory Notice 15-37. If it would be helpful to discuss our specific comments or views on any of these issues, please contact Richard Foster at Richard.Foster@FSRoundtable.org; or Felicia Smith, Vice President and Senior Counsel for Regulatory Affairs, at Felicia.Smith@FSRoundtable.org.

Sincerely,

Rich Foster

Richard Foster
Senior Vice President and Senior Counsel
for Regulatory and Legal Affairs
Financial Services Roundtable

Attachment – Appendix, FSR/BITS, *"Preventing Elder Financial Abuse"*

With a copy to:

James S. Wrona, Vice President and Associate General Counsel
Jeanette Wingler, Assistant General Counsel
Office of General Counsel

Ann-Marie Mason, Director and Counsel
Shared Services

FINRA

APPENDIX

THE FINANCIAL SERVICES ROUNDTABLE • BITS

“PREVENTING ELDER FINANCIAL ABUSE”

TABLE OF CONTENTS

BITS

FINANCIAL SERVICES ROUNDTABLE

PROTECTING THE ELDERLY AND VULNERABLE FROM FINANCIAL FRAUD AND EXPLOITATION

April 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

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 Chicago[1], 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 survey[2] of more than 5,500 older adults, 5.2% of respondents reported current financial exploitation by a family member and 6.5% reported lifetime financial exploitation by a non-family individual. 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 exploitation[3]. A 2009 report estimates the annual financial loss by victims of elder financial abuse to be at least $2.6 billion. It also describes the typical victim of elder abuse as a woman over 75 who lives alone.[4]

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

According to 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.ncjrs.gov/pdffiles1/nij/grants/226456.pdf*.
[3] Other categories tracked by NAPSA included physical, sexual, and emotional abuse, neglect (including self-neglect), abandonment, and information about scams, proposed legislation, community meetings, etc.
[4] *Broken Trust: Elders, Family, and Finances*, MetLife Mature Market Institute; produced in conjunction with the National Committee for the Prevention of Elder Abuse and Virginia Tech, *http://www.metlife.com/assets/cao/mmi/publications/studies/mmi-study-broken-trust-elders-family-finances.pdf*.
[5] *The State of Aging and Health in America,* Centers for Disease Control and Prevention (CDC) and The Merck Company Foundation, 2007, *http://www.cdc.gov/Aging/pdf/saha_2007.pdf*.
[6] The National Center on Elder Abuse, http://www.ncea.aoa.gov/ncearoot/Main_Site/index.aspx.

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 laws[8] 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 exploitation[9].

Financial institutions are encouraged to broaden dialogue with and report suspected fraud to Adult Protective Services (APS), as required by law[10]. 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" J*ournal 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 abuse[11]. 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 fraudsters[12] and employ monitoring and access controls to prevent them from unnecessarily accessing customers' records, some employees may abuse their relationships or use their knowledge of internal processes to steal from their elderly customers.

- **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.

- 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.

- 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,*

  - 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 FBI[15] or USSS[16] 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 handbook[20] 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 listserve 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://bewiseonline.org.

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

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

Fiduciary Abuse Specialist Team (FAST) – The Los Angeles FAST team was developed to provide expert consultation to local APS, Ombudsman, Public Guardian and other 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 Deposit Insurance Corporation (FDIC) – The Federal Deposit Insurance Corporation publishes the FDIC Consumer News quarterly to help people protect and stretch their money. The Fall 2005 edition of "Fiscal Fitness for Older Americans: Stretching Your Savings and Shaping Up Your Financial Strategies" included a section on frauds targeting the elderly. For more information, see http://www.fdic.gov/consumers/consumer/news/cnfall05/index.html.

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

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

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

MetLife Mature Market Institute® (MMI) – The MMI site offers pamphlets, guides and tip sheets designed to assist decision-makers about retirement planning, caregiving and healthcare. Such publications include *Helpful Hints: Preventing Elder Financial Abuse*[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,

[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

http://www.nasaa.org/Investor_Education/NASAA_Fraud_Center/, contains resources and information to protect against investor fraud.

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 Enslen, BBVA Compass
Vivian Richardson, BBVA Compass
Teresa Steele, BBVA Compass
Dianne Shovely, 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/.

THE FINANCIAL SERVICES ROUNDTABLE 

Older Americans Financial Abuse Prevention Working Group

June 2012

Included in this booklet are links to programs on financial literacy and fraud prevention as well as an overview of tips for older Americans.

Financial Literacy Programs

Ameriprise Financial, Inc.

Resources for Senior Investors and Vulnerable Adults

www.ameriprise.com/customer-service/senior-investors.asp

CFP Board

Consumer Guide to Financial Self-Defense

www.cfp.net/learn/FinancialSelfDefense/RedFlag10.asp

Lifelong Financial Strategies: 25 Tips over 25 weeks

www.cfp.net/learn/lifestage3.asp#link11

Federal Trade Commission

Money Matters

www.ftc.gov/moneymatters

Financial Literacy and Education Commission

Planning for Retirement / Retiring

www.mymoney.gov/category/topic1/planning-retirement/-retiring.html

Institute for Financial Literacy

Senior Financial Safety

www.financiallit.org/programs/distancelearning.aspx

Social Security Administration

When to Start Receiving Retirement Benefits

www.socialsecurity.gov/retirementpolicy/retirement-security.html

U.S. Department of Labor

Taking the Mystery Out of Retirement Planning

www.dol.gov/ebsa/Publications/nearretirement.html

Women's Institute for a Secure Retirement & National Council on Aging

Savvy Saving Seniors: Steps to Avoiding Scams

http://www.wiserwomen.org/index.php?id=661&page=Financial_Elder_Abuse_Resources

Wells Fargo & Company

Having a Conversation … With Your Parents

www.wellsfargo.com/beyondtoday/ages-stages/conversations/parents

Guide to Financial Protection for Older Investors

https://saf.wellsfargoadvisors.com/emx/dctm/Marketing/Marketing_Materials/Retirement_Planning/e6540.pdf

Tips for Staying Financially Fit

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

Determine the appropriate products for you. Institutions offer a wide variety of products to respond to consumer needs. Investigate the products and determine which will benefit your lifestyle.

Plan for your estate. To assist your family when decisions must be made, it is helpful to have the following legal documents: a durable power of attorney in the case of incapacity, living will for health care decisions, and a will for property distribution decisions. Many communities offer free or low cost legal services for seniors. Contact your local Area Agency on Aging for a referral or call 1-800-677-1116.

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

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

National Foundation for Credit Counseling
1.800.388.2227
www.nfcc.org

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

Consumer Credit Counseling Service
1.800.388.2227
www.cccsatl.org

Contact your local Area Agency on Aging or call 1-800-677-1116.

Check your credit report regularly. If you notice something wrong, contact the credit reporting company and business. Visit www.AnnualCreditReport.com or call 1-877-322-8228, the only authorized website for free credit reports. You will need to provide your name, address, Social Security number and date of birth to verify your identity.

Financial Abuse Prevention Programs

American Bankers Association
Protecting the Elderly from Financial Abuse
www.aba.com/aba/documents/statementstuffersamples/ElderAbuse.pdf
Compliance Course for Institution Employees
www.aba.com/eLearning/EL_RCElderFinAbuse.htm

BancWest Corporation
Financial Elder Abuse Prevention Efforts
www.fsround.org/fsr/pdfs/fin-lit-corner/BOTWsCommitmenttoPreventingFinancialElderAbuse20.pd

BITS
Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation
www.bits.org/publications/fraud/BITSProtectingVulnerableAdults0410.pdf

Capital One Financial Corporation
MoneyWi$e: Elder Fraud
www.money-wise.org/modules/module_elder_fraud

Consumer Action
Elder Fraud
http://www.consumer-action.org/english/library/C35

Comerica Incorporated
Financial Literacy Programs
www.fsround.org/fsr/pdfs/fin-lit-corner/ComericaIncorporated.pdf

Federal Bureau of Investigation
The Grandparent Scam
www.fbi.gov/news/stories/2012/april/grandparent_040212

Federal Trade Commission
10 Things You Can Do to Avoid Fraud
www.ftc.gov/bcp/edu/pubs/consumer/general/gen23.pdf

PA Department of Aging's Institute on Protective Services at Temple University
Task Forces
www.instituteonps.org

TD Bank
Identity Theft / Elder Abuse Presentation
www.fsround.org/fsr/pdfs/fin-lit-corner/fraudprevention.pdf

Wells Fargo & Company
Suggestions for Seniors
www.handsonbanking.org/library/en/Suggestions%20for%20seniors.pdf

Fraud Prevention Suggestions for Organizations Working with Older Americans

Develop publications and trainings for staff on identification of abuse and how the institution can help.

Focus education on specific schemes targeting this population (e.g., Grandparent scam, power of attorney abuse, contractor frauds).

Interact with Key Partners

Consider offering educational events with partners (e.g., law enforcement, Adult Protective Services) to reach out directly to individuals at senior centers or community groups (e.g., Rotary, Kiwanis).

Conduct outreach to law enforcement, local hospitals, specifically geriatric practitioners, local Adult Protective Services, and other businesses such as CPA firms.

Work as a team to respond to customer and staff concerns related to diminished capacity or financial abuse of this customer category.

Encourage staff to report suspected abuse. Staff may be able to notice signs of abuse. Instances of suspected abuse should be reported to Adult Protective Services.

Report suspicious activity to the appropriate internal entity to submit reports to Adult Protective Services. The U.S. Administration on Aging's National Center on Elder Abuse has a site outlining state specific information. www.ncea.aoa.gov/NCEAroot/Main_Site/Find_Help/State_Resources.aspx

Create or participate in efforts' that include representatives from prosecutors, attorneys, Adult Protective Services, law enforcement, social service agencies health care providers, senior care agencies, ombudsman offices and financial institutions. A local example includes:

- SAVE (Serving Adults who are Vulnerable and /or Elderly) in Oakland County, Michigan www.oakgov.com/seniors/elder_abuse/

Fraud Prevention Tips for Consumers

Choose a trusted individual when providing power of attorney. Your attorney can discuss the benefits of appointing a power of attorney so someone can make decisions on your behalf when you are no longer able. Carefully review the authority the power of attorney document grants your designee, especially regarding the ability to make gifts.

Stay active and engage with others regularly. Fraudsters prey on individuals who have infrequent contact with others.

Respond cautiously to in-person, mail, Internet or solicitations. Discuss with a trusted friend or family member any deal that sounds too good to be true. For instance, you can't win a lottery, if you haven't entered.

Know that wiring money is like sending cash. Con artists often insist that people wire money, especially overseas, because it's nearly impossible to reverse the transaction or trace the money. Don't wire money to strangers, to sellers who insist on wire transfers for payment, or to someone who claims to be a relative in an emergency.

Contact the institution if a request looks suspicious. Fraudsters may contact you purporting to be your institution. Before providing any information, contact the institution through your regular channels (e.g., in-person visit, phone call) to confirm the request is from the institution.

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

Don't let embarrassment or fear keep you from discussing suspicious activities. The situation could become worse if not escalated. Discuss any suspicious activity with someone you trust (e.g., family member, bank manager, attorney, local Area Agency on Aging, police).

Monitor your financial affairs. Actively track your financial accounts so you will be able to quickly recognize when a fraudulent transaction appears.

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

Don't deposit checks you receive from strangers. Fraudsters may ask you to deposit a check and then require you to send a portion back. Ask your institution for help to prove the legitimacy of a check before you send any money to a stranger.

Educate yourself on the products offered by your institution. Contact your institution or the local Area Agency on Aging to request educational information on financial products. Many financial institutions offer resources to explain these.

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

To locate the Area Agency on Aging in your community call 1-800-677-1116.

Participants:

American Bankers Association
American Bar Association Commission on Law and Aging
Ameriprise Financial, Inc.
BancWest Corporation
Bank of America Corporation
BMO Financial Corp.
Capital One Financial Corporation
Certified Financial Planners Board of Standards
Comerica Incorporated
Credit Union National Association (CUNA)
Employee Benefits Research Institute
Fidelity Investments
PA Department of Aging's Institute on Protective Services at Temple University
JPMorgan Chase & Co.
KeyCorp
M&T Bank Corporation
Montgomery County State's Attorney's Office
National Adult Protective Services Association (NAPSA)
National Endowment for Financial Education
Oklahoma Bankers Association
Philadelphia Corporation for Aging
People's United Bank
The PNC Financial Services Group, Inc.
RBC Capital Markets
RBS Americas (Citizens Financial Group, Inc.)
Regions Financial Corporation
SunTrust Banks, Inc.
TD Bank
U.S. Bancorp
University of Maryland
Wells Fargo & Company
Women's Institute for a Secure Retirement (WISER)

STATEMENT

OF

BITS PRESIDENT PAUL SMOCER

ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

SPECIAL COMMITTEE ON AGING

OF THE U.S. SENATE

AMERICA'S INVISIBLE EPIDEMIC:

PREVENTING FINANCIAL ELDER ABUSE

NOVEMBER 15, 2012

The Financial Services Roundtable[1] (the "Roundtable") and BITS appreciate the opportunity to share our thoughts with the members of the Senate Special Committee on Aging regarding the financial exploitation of older Americans and actions we can collectively take to reduce that exploitation.

The financial services industry is a key part of the circle protecting older Americans from financial fraud and exploitation. When employees observe signs of potential exploitation, they can work with families, caregivers, social service agencies and law enforcement to prevent, detect, and help investigate and prosecute the individuals who engage in fraud.

The Roundtable and its members are committed to encouraging their employees comply with high standards of conduct when providing financial advice to all customers, including older Americans and their families. Helping ensure a secure retirement for millions of Americans is central to the business and the mission of the financial services industry.

THE PROBLEM

By 2030, the number of Americans aged 65 and older is projected to double to 71 million, roughly 20 percent of the U.S. population.[2] In some states, fully a quarter of the population is likely to be aged 65 and older.[3] Unfortunately, this increase in the aging population creates a potentially large pool of potential victims for financial exploitation.

It is sad, but true, that the most frequent perpetrators of financial abuse are family members, who by some estimates commit nearly 75% of crimes,[4] and professional criminals. It is also important to note that financial institutions are often the first line of defense against this financial exploitation.

Since many older customers prefer to conduct transactions in person, financial services employees can be the first to detect changes in an older customer's behavior. Signs of exploitation of an elderly customer may include unusual transactions or changes to accounts, unpaid bills, changes in spending patterns, new individuals accompanying the customer to a bank facility, and missing property. When these and other signs are detected, and an investigation suggests that exploitation is taking place, financial institutions can help the

[1] The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America's economic engine, accounting directly for $85.5 trillion in managed assets, $965 billion in revenue, and 2.3 million jobs.

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

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

[4] http://www.consumerreports.org/cro/money/consumer-protection/preventing-financial-elder-abuse/overview/index.htm

customer take action to protect his or her assets. Financial institutions also work with agencies such as Adult Protective Services (APS), local law enforcement and prosecutors, many times as part of local or regional task forces focused on elder abuse prevention and prosecution. Institutions also report suspected abuse via the Suspicious Activity Reports (SARs) filed with the Financial Crimes Enforcement Network (FinCEN), an agency of the United States Department of the Treasury.

Following the filing of SARs, institutions may be contacted by law enforcement who are investigating the case. Institutions actively work with law enforcement after filing all legally required documents. Institutions also participate in regional partnerships that involve law enforcement of all levels. During these meetings, institutions will share trends and suspects. This allows for institutions and law enforcement partners to share best practices. Through this active engagement and partnership, cases are able to be more quickly resolved.

For decades, financial institutions have been at the forefront of fraud detection utilizing sophisticated technology, modeling, training and education. Because of these proactive measures, they are often the first to detect patterns associated with fraud. Using a variety of safeguards, financial institutions make every attempt to ensure the reliability and security of financial transactions as well as protect financial privacy. In fact, financial institutions often exceed the standards set by financial regulators in order to protect their customers, shareholders and employees better.

Education – of employees, customers and other stakeholders – is critical for preventing financial abuse of all customers – including more vulnerable ones such as older Americans. Many financial institutions have extensive programs to educate employees and customers on detecting abuse and steps to secure accounts from the lure of fraudsters. Financial institutions also work closely with APS, law enforcement and prosecutors to educate those entities on patterns of fraudulent activity and help identify individual cases of potential fraud. Financial institutions also work closely with community organizations to host panel discussions and community events to educate seniors and their caregivers about the risk of elder financial abuse. These efforts provide older American and their advocates education and resources to not only recognize financial elder abuse, but to also take steps to proactively protect oneself and ones assets through, for example, proper document disposal and identity theft prevention, and reports of the crime when it occurs.

Employees and customers who are better educated about fraudulent behavior and preventing fraud are more likely to take fraud prevention measures. An example of the Roundtable member's education efforts is a white paper produced by the Roundtable's BITS group entitled, "*Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation,"* which helps financial institutions and their customers identify and combat elder abuse.[5]

[5] BITS - "Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation"

The Roundtable also partnered with the Administration for Community Living/Department of Health and Human Services and the Consumer Financial Protection Bureau to support the June 14, 2012 White House Office of Public Engagement symposium in recognition of the 7th annual World Elder Abuse Awareness Day by providing financial industry speakers for the panel addressing the prevention of elder financial abuse.

Recognizing the scope of this issue, the Roundtable's member believe it is important to continue to focus on it and to bring resources to bear. To that end, the Roundtable's members have formed a working group to focus on the issue of preventing financial abuse of the elderly. Further recognizing that solutions will require a multi-faceted approach, the Group's members consist not only of financial institutions, but additionally of a collaborative cross-section of federal agency representatives, representatives from various adult protective services organizations, and academics focused on the area of elder abuse.

The Elder Working Group currently has identified two key projects on which it will concentrate. These are:

- Develop a structure/syllabus for training financial institution consumer-facing staff and all new hires on elder fraud trends and internal procedures for reacting to suspected elder financial abuse, including engaging Adult Protective Services and law enforcement. This work will focus on building on work done previously, will incorporate new learnings and research and broaden the educational base for employees. Once completed, the work will be shared openly across the financial services sector.
- Work with financial institutions with strong education programs to develop a publicly available awareness and education program to be made available to all financial institutions.

CHALLENGES AND IMPEDIMENTS

As we have engaged in our efforts regarding prevention of elder financial abuse and based on the experiences and feedback of financial institutions, we have identified a number of areas where potential impediments exist to improving prevention. For many of those, the assistance of the agencies forming the Elder Justice Coordinating Council (EJCC), either directly or in concert with other non-EJCC agencies, would be helpful to clarify concerns or remove impediments. On October 11, 2012, I had the opportunity to present these ideas to the agencies involved in the EJCC at its inaugural meeting. The impediments and possible solutions include:

- Clarify the permissibility of age-based fraud monitoring. As noted previously, financial institutions utilize sophisticated fraud detection technology and modeling in their attempts to prevent and identify potential fraudulent activity in an attempt to protect customers. An added layer of sophistication could be to segregate their elder customers' activities for special screening. Many financial institutions are concerned, however, that segregating their customer population for this purpose could be

interpreted to place them in violation of existing age discrimination laws and, therefore, put the institution at risk for potential fines or regulatory actions.

It would be extremely beneficial if the involved EJCC agencies, particularly the Department of Justice, could clarify permissibility of age-based fraud monitoring. If such segregation is currently permissible, to assuage the concerns we have heard, a written opinion of the permissibility would be extremely helpful. If, in fact, it is considered a violation of current anti-discrimination laws to segregate this population for fraud monitoring purposes, we encourage the EJCC to undertake an effort to pursue legislative action to allow for an exception.

- Authority to authorize a protective hold on a suspicious transaction. One significant challenge financial institution employees encounter is situations where an elderly customer wants to perform a transaction (e.g., a withdrawal, a request to transfer funds) in a situation where the employee strongly suspects or even knows that fraud is involved. This clearly creates a conundrum pitting the financial institution's contractual obligation to carry out its customers and instructions and the financial institutions' desire to prevent the elderly customer from being defrauded.

  There are a few methods that are suggested for dealing with this issue:
  - Working with CFPB and Treasury create an option allowing institutions to put a minimal hold on the transaction pending the sending of an alert of APS and APS discussing the situation with the customer. It will likely be necessary for CFPB and Treasury to work with the states to implement this suggestion.
  - Working collaboratively with input from the U.S. Department of Justice, U.S. Postal Inspection Service, Federal Trade Commission and other agencies along with input from financial institutions, create and maintain a list of known fraudulent actors that can be used to "convince" elders of their involvement in a fraudulent situation.
  - Leverage the work already underway and led by the Consumer Financial Protection Bureau to create a list of local and regional APS services into a shareable database that financial institutions could use to understand who to contact that might be helpful in discussing these types of situations with involved elders. Along with creating a database for contacts, it will be necessary to further clarify the type of information institutions are legally able to share with APS regarding their older customer.

- Another substantial challenge occurs when an individual with a duly executed Power of Attorney to act on behalf of an elder is suspected of trying to perpetrate fraudulent activity or activity not in the best interest of the elder. Duly executed Powers of Attorney give the holder the legal right to act on behalf of the customer. This essentially creates the same conundrum for the financial institution as noted in the previous point.

There are a series of actions we would ask the EJCC members to consider regarding this issue. They include:

- Powers of Attorney laws and regulations vary by state and, particularly in the case of Durable Powers of Attorney, can involve granting rights to the agent even after the principal becomes incapacitated. While the agent is obligated to exercise due care and protect the principal, state law is not uniform with respect to the specific responsibilities of an agent with regard to financial transactions, particularly when the principal is an elder. The development of uniform state laws and a Uniform Power of Attorney would be very helpful. Study of the feasibility and benefits of having a uniform Power of Attorney, particularly one for situations in which the principle is an elder should be undertaken.
- Select agencies – most likely U.S. Department of Health and Human Services, Social Security Administration, CFPB, U.S. Department of Justice, the Federal Trade Commission and the U.S. Department of Veterans Affairs – should consider working collaboratively to develop educational materials that explain clearly to those agents with Powers of Attorney their financial responsibilities and provide specific examples of what are considered abusive behaviors.
- The U.S. Department of Justice could undertake a study of existing criminal statutes that apply to financial abuse of elders. This should include both federal and state level statutes with the goal to develop a model criminal code applicable to this area that strongly disincents criminal actors and those acting as agents from taking advantage of the elderly.

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

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

- Confusion of requirements regarding to whom to report the abuse and under what circumstances.

FinCEN, a part of the U.S. Treasury, issued an advisory on February 22, 2011 that addresses the reporting of actual or suspected elder financial abuse on Suspicious Activity Reports (SARS).[6] This provided financial institutions with guidance on reporting specific to SARs' requirements; however, the reporting of elder financial abuse often goes beyond that type of reporting. Reporting would likely include reporting of situations to Adult Protective Services or similar agencies as well potentially, depending on the circumstances, to local law enforcement. Today, however, the structure of adult protective services type agencies is diffused across the country. Some locations have more centralized statewide or regional agencies will others structure such agencies very locally. Determining the correct agency for reporting is often difficult. Law enforcement capabilities to deal with such reports often vary as well. In addition, today with law enforcement often done at the local level, it is often difficult to synthesize information across jurisdictions to identify when elders in different locations may be being subjected to scams and fraudulent activity that relates to the same set of criminal actors.

To assist with overcoming these issues, we suggest the following actions:

- The CFPB is currently working with various constituencies to develop a database of regional and local Area Agency on Aging across the United States. Making that database accessible to financial institutions would facilitate those institutions ability to know and contact the correct agency.
- Recognizing that local law enforcement lacked skills in investigating cybercrime, in 2007, the Department of Homeland Security, the United States Secret Service, the Alabama District Attorneys Association, the State of Alabama, and the city of Hoover, Alabama partnered to create the National Computer Forensics Institute (NCFI). This partnership provides state and local law enforcement officers the training necessary to conduct basis electronic crimes investigations. Creating a similar model to train state and local law enforcement personnel the training necessary to conduct investigations of elder abuse could have significant merits. Short of such a large effort, creating and providing to local law enforcement bodies an educational opportunity through such options as written best practices, webinars and seminars on the subject would be beneficial.

  Note that these same concepts can be generally applied as well to local prosecutorial authorities, who sometimes also lack the knowledge and experience requisite to the successful prosecution of those who prey financially on the elderly. Similar training programs and best practices can also serve this community well.
- The CFPB is currently working to establish state and regional coalitions of APS, law enforcement, prosecutors and financial institutions that can work together on the issue of elder abuse. We encourage continued expansion of this effort

[6] See http://www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html.

and offer our services to assist in connecting our Roundtable members into these coalitions.

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

- Enhanced financial literacy to empower further consumers, including older Americans, to make sound financial decisions.

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

  As we noted earlier, as a part of the efforts of its Elder Working Group, the Roundtable has committed to work on two projects (i.e., develop a structure/syllabus for training financial institution consumer-facing staff and to develop a publicly available awareness and education program to be made available to all financial institutions).

  We would certainly welcome the engagement of any of the departments or agencies represented on the EJCC in this effort – either in development or ultimately in distribution of the publicly facing awareness and education materials developed. We believe a national-level awareness campaign targeting elder Americans and their family members would provide long-lasting benefits in helping to reduce elder financial abuse.

- One last area of potential improvement involves the licensing of financial professionals who serve the elder community. In its August 20, 2012 letter to the CFPB regarding CFPB's "Request for Information Regarding Senior Financial Exploitation [Docket CFPB-2012-0018]," the Roundtable mentioned another key area to reduce financial abuse of elders. It noted that an effort to make elders more aware of the licensing of financial professionals coupled with an effort by federal and state agencies and professional organizations' role in developing best practices for the training and licensing of financial professionals would have benefits. The Roundtable's comments on this last area are excerpted into Appendix A of this document.

CONCLUSION

We appreciate the opportunity to share our sector's focus on the issue of financial abuse of the elderly. We are committed to continuing to work on these issues to protect older Americans.

As noted, we recently shared these thoughts with the Elder Justice Coordinating Council. The challenge of reducing elder abuse can only be resolved by continued focus on the issue by all relevant parties, including financial institutions, families of elders, government agencies and

legislators. Only through this continued commitment will we be able to protect our seniors from financial abuse. We recognize that the ideas we have outlined in this testimony are, in many cases, concepts and suggestions. They are a starting point for this discussion. We recognize there are various methods to approach these issues and look forward to continuing to work with you and other key constituencies on these issues.

Appendix A

Excerpt from August 20, 2012 letter to the CFPB regarding CFPB's "Request for Information Regarding Senior Financial Exploitation [Docket CFPB-2012-0018]

- **Consumers Should Seek Financial Advice Only From Licensed Financial Professionals, and the CFPB Should Work with Federal and State Agencies and Professional Organizations to Develop Best Practices For the Training of These Professionals**

The financial services industry has played a vital role in expanding retirement security for millions of Americans for the last 100 years. The industry currently manages more than $17 trillion in retirement assets, which represents 36% of all U.S. household assets.[7] The U.S. retirement market is projected to grow to nearly $22 trillion by 2016,[8] a 30% increase in retirement savings over four years.

It is important that consumers of all ages seek professional assistance to prepare for and make major financial decisions involving investments, wealth planning, and retirement. When making these decisions, consumers should seek out individuals who are licensed under federal and/or state law.

The Roundtable believes that consumers should only hire properly licensed investment professionals. Federal law regulating securities brokers, securities dealers, and investment advisers provides strong and effective protection for all consumers, including older Americans. The Securities and Exchange Commission, together with securities self-regulatory organizations like the Financial Industry Regulatory Authority (FINRA) and the Municipal Securities Rulemaking Board, implement the registration and regulatory régime under federal securities law. These protections are complemented at the state level by laws designed to protect consumers from investment fraud. A similar registration and regulatory structure exists for futures professionals and firms, which are subject to oversight by the Commodity Futures Trading Commission, National Futures Association and other futures self-regulatory organizations. Additionally, state insurance commissioners regulate insurance agents in their respective jurisdictions.[9]

[7] http://www.ebri.org/research/?fa=genretire

[8] http://www.bankinvestmentconsultant.com/news/cerulli-predicts-retirment-market-will-exceed-22-trillion-by-2016-2677132-1.html

[9] The most common license for securities professionals is the Series 7 – General Securities Representative, and the most common license for commodity futures professionals is the Series 3 – National Commodity Futures. Depending on the nature of their activities, investment professionals may need the following licenses: (1) Series 6 – Investment Company Products/Variable Contracts Limited Representative; (2) Series 22 – Direct Participation Programs Limited Representative; (3) Series 31 – Futures Managed Funds; (4) Series 32 – Limited Futures; (5) Series 34 – Retail Off-Exchange Forex; (6) Series 42 – Registered Options Representative; (7) Series 52 – Municipal Securities Representative; (8) Series 62 – Corporate Securities Limited Representative; (9) Series 63 – Uniform Securities Agent State Law (NASAA); (10) Series 65 – Uniform Investment Adviser Law (NASAA); (11) Series 66 – Uniform Combined State Law (NASAA); and (12) Series 82 – Limited Representative, Private Securities Offerings.

We understand that a number of states and professional organizations have laws and programs that govern certifications and titles used by retirement professionals. While training that focuses on the specialized needs of older Americans may be valuable and useful, we urge the CFPB to partner with the financial services industry, federal regulators, financial industry self-regulatory organizations, state agencies and professional organizations in developing best practices for the training and certification of professionals who specialize in advising older Americans.

THE FINANCIAL SERVICES ROUNDTABLE

Financing America's Economy

BITS

FINANCIAL SERVICES ROUNDTABLE

At-Risk Adult Training Curriculum

February 2013

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

At-Risk Adult Training Curriculum

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

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

This document covers the following:

Developing an Internal Training Seminar

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

Additional Training for Fraud Investigators

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

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

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

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

About The Financial Services Roundtable/BITS

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

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

Developing an Internal Training Seminar

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

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

Content

1.0 Background

1.1 Definitions

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

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

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

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

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

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

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

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

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

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

1.2 Legal Obligations

1.2.1 FinCEN Filings

1.2.1.1 February 2011 FinCEN Advisory

1.2.2 State Requirements

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

1.3 Role of the Financial Institution

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

1.3.2 Report suspicious activities to FinCEN.

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

1.4 Stories of experiences

1.4.1 Provide examples of recent cases.

1.4.1.1 Family Fraud

1.4.1.2 Gold Investment Scheme

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

1.4.3 Oklahoma Bankers Association "Senior Cents" Video

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

2.0 Fraud Schemes[3]

2.1 Categories of Exploiters

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

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

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

3.0 Suspicious behaviors

3.1 Visual Cues

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

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

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

3.1.4 Secretive or giving implausible explanations for use of funds.

3.1.5 Unable to remember financial transactions or signing paperwork.

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

3.1.7 Isolated from other family members or close friends.

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

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

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

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

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

6.0 Discussion of successful identification of perpetrator.

Additional Training for Fraud Investigators

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

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

9.0 Collect and document surveillance videos and photos.

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

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

12.0 State Compliance Requirements

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

Appendix A: For Senior Customers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Consumer Credit Counseling Service
1.800.388.2227
www.cccsatl.org

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

Appendix B: For Family Members and Fiduciary

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

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

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

Watch for signs of mental changes or abuse.

Diminished mental capacity

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

Third Party Financial Abuse

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

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

Appendix C: For Financial Institution Staff

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

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

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

Use probing questions. Specific questions will help determine the customer's intent. It is important to let the customer express their intent using his or her own words without prompting. For example, when finalizing a power of attorney "Mr. Jones, do you want Ms. Smith to be able to withdraw money from your account at any time without needing your permission?" Or when someone accompanies an elder to your institution and you suspect the potential that the person is influencing the elder, you might privately ask, "Mr. Jones, are you sure you want to do this transaction?" and explain the effect of the transaction.

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

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

Diminished mental capacity

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

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

- Diminished hearing
- Diminished vision
- Memory loss

Third Party Financial Abuse

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

WORLD ELDER ABUSE AWARENESS

The United Nations has designated June 15 as World Elder Abuse Awareness Day. This day's aim is to focus attention on the issue of physical, emotional, and financial abuse of elders.

The U.S. Census reports that by the year 2050, people over age 65 will make up approximately 20 percent of the population. Fighting elder fraud is not a competitive issue for FSR members – it's a duty.

Find out below what the financial services industry is doing to encourage others to recognize the problem of elder abuse and create policies that prevent people from taking advantage of our older generations.

Refuse Elder Abuse: FSR Members Thwart Fraud Perpetrators

Fraud and financial abuse schemes targeting the elderly are a growing problem in the United States that cost victims at least $2.9 billion in 2010 alone.

With the evolution of technology, criminals are finding new ways to target the money of vulnerable consumers. The Financial Services Roundtable's member companies are leaders in the elder fraud prevention field, working around the clock to aggressively identify red flags and hinder illicit criminal activity.

According to the Scam Awareness Alliance, popular corruption schemes include Romance Scams, where older, often lonely Americans conned into wiring money to an anonymous love interest they've met online. Other scams include Lottery Scams and Person-in-Need Scams, which are featured in the alliance's series of online ads.

Why is the elder population the bulls-eye for fraudsters? Wells Fargo Advisors (WFA), a non-bank affiliate of Wells Fargo & Company, notes that the elder population is typically more trusting, likely to spend time alone, often inclined to answer their door and phone at home and are hesitant to report suspected fraud. Not only does Wells Fargo Advisors, provide guidance

for the financial protection of older investors**,** but the bank is also at the forefront of collaboration, halting fraud before it occurs. WFA is gearing up to announce the development of a new division of 15,146 advisors represented from all 50 states, allowing elder financial abuse cases flow through a centralized point, enhancing the investigation and reporting process to state Adult Protective Service departments.