Aging and Exploitation:
How Should the Financial Service Industry Respond?

Marguerite DeLiema and Martha Deevy

Prepared for presentation at the
Pension Research Council Symposium, May 5 - 6, 2016
"Financial Decision Making and Retirement Security in an Aging World"

Aging and Exploitation:
How Should the Financial Service Industry Respond?

Marguerite DeLiema & Martha Deevy

Abstract

Elder financial exploitation, including scams that target seniors and financial abuse by friends and family, is a growing problem facing older Americans. At its core, financial exploitation involves a transfer of funds from a victim to a perpetrator, and as the nodes from which this money leaves the client's hands, financial service firms are positioned to stop financial exploitation at its source. They may be first to notice declines in their clients' decision-making capacity and to observe losses from their bank or investment accounts. In this chapter, we present innovative ways that wealth advisory firms and retail banks are addressing the problem. We interview representatives at small and large firms to learn about their financial exploitation training and prevention programs, their detection and response protocols, and how they balance the goals of client protection with privacy and the client's right to autonomy in financial decision-making. We also interview representatives from financial service regulatory agencies to describe what interventions firms are authorized to do to when they suspect elder financial exploitation, the legal barriers they face, and recent rule change proposals that may overcome some of these barriers. By identifying suspicious activity early, halting fraudulent transactions, involving social services and law enforcement agencies, and alerting the client's friends or family members, financial service firms can minimize the risk of elder fraud and financial abuse.

Keywords: Elder financial exploitation, financial advisor, fraud prevention, fraud detection, elder financial abuse, financial planning

Introduction

Elder financial exploitation—which encompasses fraud targeting vulnerable older adults and elder financial abuse by someone in a position of trust—is difficult to define. This is partly due to the diverse mechanisms of financial exploitation, the various actors involved, and the different types of relationships between perpetrators and their victims (Jackson 2015). The National Center on Elder Abuse (1998) defines elder financial exploitation as the illegal or improper use of an elder's funds, property, or assets. An 'elder' is typically defined as an adult over the age of 60 or 65, although legal statutes and social programs for the elderly often use different designations.

Financial exploitation includes crimes such as scams and fraud, use of an older person's checks, credit or debit cards without permission, wrongful transfer of property or assets, misappropriation of funds, and abuse of fiduciary duty by a trusted representative (Bonnie & Wallace 2003). Friends, relatives, and caregivers who financially abuse a vulnerable older person take advantage of that person's trust to gain control of bank accounts, check books, and payment cards, often under the guise of 'helping' the elder manage his finances. The abuser may be an appointed power of attorney, a legal guardian, a trustee, or someone else in a fiduciary role; or have access to the elder's money simply due to a long-standing social bond. Fraud perpetrators, by contrast, are predatory strangers who must earn an elder's trust by promising a future benefit or reward in exchange for money or personal information upfront.

Compared to younger age groups, seniors may be disproportionately targeted by fraud perpetrators based on assumptions that they are more trusting of strangers, socially isolated, cognitively impaired, and have more financial resources to exploit. Older adults' generally have higher credit scores and more established saving accounts, also making them more attractive

targets for identity thieves and hackers (Comizo et al. 2015), yet people of all ages can be victims of fraud regardless of cognitive status or financial sophistication. Common scams targeting seniors include bogus sweepstakes and prize promotions, unnecessary health care products, imposter scams, bogus investments, tech support scams, and fake charities (National Council on Aging 2015). To elicit compliance, perpetrators use tactics such as false affiliation with a trusted authority, social consensus, emotional arousal, enticement, intimidation, undue influence, and other persuasion methods. Victims ultimately never receive the promised rewards because they do not exist, were never intended to be provided, or were grossly misrepresented (Titus et al. 1995). In this paper we focus on *financial abuse* where an older victim was exploited by friends and/or family members (people in positions of trust), and also *elder fraud* where a vulnerable older adult willingly agreed to give the perpetrator money in exchange for a promised future benefit or reward. Crimes in which the victim had no active role in the fraudulent transaction or where there was no interaction with the perpetrator at all—such as credit card theft or identity theft—are outside the scope of this chapter.

As the number of adults ages 65 and older grows in the United States, so will the incidence and cost of financial exploitation. A study by Kristy Holtfreter and colleagues (2014) found that prevalence of elder financial fraud in the past year was approximately 14% among those age 60 and older in Florida and Arizona (Holtfreter et al. 2014). This is higher than rates of elder financial abuse by a family member in the past year: 5.2 percent among community-residing adults age 60 and older (Acierno et al. 2010), although it's likely that both numbers are underestimates given the low rates of reporting among older people (Pak & Shadel 2011). Conservative estimates of direct losses from elder financial exploitation are $2.9 billion a year (MetLife Mature Market Institute 2009). Total losses for all US adults may be well over $50

billion annually (Deevy & Beals 2013). In addition to direct losses, other costs include legal fees and taking time off work to resolve the incident; and emotional consequences such as shame, frustration, depression, and feelings of betrayal (Button et al. 2014; Deem 2000; FINRA Foundation 2015). Among victims who experienced indirect losses from fraud, 45 percent of survey respondents had between $100 and $1,000 in additional costs associated with the incident, and 29 percent had over $1,000 in indirect costs (FINRA Foundation 2015).

The financial industry has a pivotal role to play in protecting vulnerable clients. Financial professionals are well positioned to recognize the hallmarks of fraud and financial abuse, which include uncharacteristic withdrawals from checking, savings, or investment accounts; forged signatures on checks or financial documents; abrupt changes in powers of attorney; unexplained asset transfers; large checks written out to cash; and strangers becoming involved in the client's financial affairs (Condrad et al. 2011). Most financial professionals have witnessed these and other signs during their careers. For example, a 2012 study by the Certified Financial Planner (CFP) Board of Standards found that 56 percent of CFPs stated they had a client who had been subject to unfair, deceptive or abusive practices with an average loss of $50,000 per victim (CFP Board of Standards 2012).

Firms face increasing pressure from regulators to ramp up their fraud prevention efforts. They can suffer customer litigation liability and enforcement actions for failing to address the risk of fraud in their compliance and employee training programs (Comizo et al 2015). In the 2015 White House Conference on Aging, financial service firms were called on by the director of the Consumer Financial Protection Bureau (CFBP) to educate employees and consumers on identifying crimes against the elderly (Cordray 2015). Due to the increased scrutiny at attention around the issue, firms are beginning to invest in programs to better detect exploitation before

funds are withdrawn, and developing protocols for responding quickly and effectively if prevention attempts fail. These practices help secure their clients' assets, restore confidence in the institution, and strengthen brand value (Gunther 2016).

Though these are powerful motivators, preventing financial exploitation is fraught with risks. Regulations governing the financial service industry are designed to uphold consumers' rights to privacy and autonomy, which sometimes interfere with a firm's financial protection efforts. For example, consumers have a right to make decisions about how and where they spend and invest their money, even if these choices challenge a financial professional's advice. So although firms have relationship management and risk management reasons to intervene when fraud is suspected (Lichtenburg 2016; Lock 2016), they must also be cautious not to infringe on their clients' rights to autonomy. This means attempting to differentiate when losses are due to financial exploitation, and when they result from poor consumer decision-making in risky financial markets, which is a significant challenge given the ambiguity of most cases.

The population of US adults ages 65 and older is projected to double by 2050 (Pew Research Center 2014). With the vast demographic, technological, and market shifts in the US, how are firms preparing for the anticipated rise in elder fraud and financial abuse? The purpose of this chapter is to describe what the financial service industry is doing to adjust to an aging client population that is frequently targeted by predatory scam artists and greedy family members. We begin by describing new and progressive approaches to financial exploitation detection, prevention, and intervention at wealth advisory and banking firms, and describe the current regulatory landscape under which these firms are operating. We highlight the limitations of current regulations and practices, identify regulatory/legislative solutions, and offer recommendations for improving client protection against financial exploitation.

Methods

Semi-structured interviews were conducted with representatives from financial service firms and regulatory agencies. Findings were further informed by research from AARP Public Policy Institute's BankSafe Initiative, policy briefs, financial institution trade organizations, and academic researchers. We focus exclusively on financial advisors and depository institutions because they have frequent customer contact and cover a sizeable proportion of the older adult population with their range of customer services. Fraud prevention efforts by credit card companies, credit unions, insurance providers, money transfer businesses, and venture capital firms are not discussed in this chapter.

In selecting interview participants, our goal was to survey a range of firms that varied in size and market share to identify the scope of fraud detection, intervention, and prevention practices. Therefore, we spoke to two large banks with over 70 million customers that manage $1.8 and $2.1 trillion dollars in assets, respectively, and employ an average of 244,000 full-time employees. We also interviewed midsize regional banks that have approximately $74 billion in assets and 10,000 employees, and small community banks that have fewer than 15 branches, less than 1 billion in assets, and under 350 employees. To examine the broker-dealer side of the industry, we also interviewed large and medium sized wealth management firms. The largest had approximately two and a half trillion in assets under management and over 15,000 financial advisors, and the smallest had nearly $650 billion assets under management and a few thousand contracted financial advisors. We also sought perspectives from government regulatory bodies that oversee financial service industries, including the Financial Industry Regulatory Authority (FINRA), the Consumer Financial Protection Bureau (CFPB), and the Securities and Exchange

Commission (SEC). Interviews took place between September and November in 2015 and were conducted by telephone.

Potential participants were identified through pre-existing relationships with researchers at the Stanford Center on Longevity (SCL) and SCL's Corporate Affiliates Program and Advisory Board. Interviews were arranged by the primary contact person at each firm or regulatory agency who assisted by selecting knowledgeable members who could share their company's financial exploitation detection and prevention programs and/or who were familiar with regulatory policies governing the issue.

Questions posed to financial service firms included: (1) What is your firm doing to detect and prevent fraud and financial abuse? (2) What regulations govern your fraud detection/prevention policies? (3) How do you train your employees to recognize the signs of fraud or financial abuse by the clients' friends, family, or strangers? (4) What are your policies for reporting concerns that a client is being victimized? (5) Are there any actions you wish you could take to intervene, but can't because of regulatory/legal issues? (6) Is your firm going beyond regulatory requirements? (7) Are there any other barriers to fraud detection and intervention that you would like to share? And, (8) Do you wish you could do more?

Questions posed to state, federal, and local regulatory bodies/law enforcement agencies were: (1) Under current rules and regulations, what are [banks/wealth advisors] obligated to do to protect their clients from fraud and financial abuse? (2) Do these regulations conflict with what firms are actually doing or not doing? If so, how? (3) What would you like to see firms doing better to protect their clients against financial exploitation? And, (4) What do you see as the future of regulation in this area?

Participating organizations provided responses to each of these questions. All participants were informed that no comments would be attributed unless special permission was requested from the participant. These steps were taken to encourage the professionals to speak candidly about a sensitive topic that is typically not discussed with researchers because of concerns about brand reputation and potential liability issues.

Results

Reducing incidence of fraud and financial abuse was regarded as a key priority across the financial service sector. Interview respondents expressed similar views that the interest in elder financial exploitation has grown exponentially in the last few years, particularly when referrals to compliance departments increased and frontline staff sought guidance from company leadership on how to address elder fraud and financial abuse situations. A major difference between the banking and wealth advisory sectors, however, is that approaches for resolving financial exploitation differ based on the firm's customer relationship model and the relevant laws. Financial advisors have personal relationships with their clients and often work with the same individual for decades and through multiple life stages. They are therefore more familiar with their clients' finances, risk preferences, and their short and long-term financial goals. Alternatively, bank employees have a transaction-based relationship with customers. Although frontline staff frequently engage with those they serve, interactions are typically very brief and are not focused on helping the customer with financial planning. Employees of small community banks may know some customers personally, but employees of large national banks have thousands of customers who patronize multiple branches across different locations. These vaying client relationship models have produced somewhat different strategies for detecting and

preventing financial exploitation, although many practices are similar across all sectors of the industry.

Borrowing terms used to classify the stages of patient care, financial exploitation can be addressed using *primary* and *secondary* intervention. *Primary* interventions focus on stopping losses before they occur, such as by blocking suspicious transactions, training frontline staff to recognize red flags, and educating customers about avoiding scams and how to shore-up assets through estate planning. The primary interventions that we discuss in this chapter include: (1) employee training, (2) community outreach, (3) early financial planning, (4) innovative financial tools and products, (5) safe financial fraud monitoring, and (6) data-driven fraud detection strategies.

Secondary interventions are for 'treating' the problem once it has already occurred, such as restitution of lost funds and/or criminal prosecution of offenders. The secondary interventions that we discuss include: (1) federal reporting of elder financial exploitation scen, (2) reporting to adult protective services (APS), and (3) working with local law enforcement agencies. Because many intervention approaches differ between banks and wealth advisors due to different client relationship models and different regulations, their unique approaches are presented separately below.

Primary interventions.

Training financial advisors.

Training wealth advisors on issues related to elder financial exploitation is required at all the firms we interviewed, although the focus, frequency, duration, and modality of training programs differed. All businesses require new employees to be trained on identifying the signs of

financial exploitation and the steps to take if exploitation is suspected. Some firms require employees to complete training one time only, generally when they are first hired, whereas others require re-training each year or whenever new guidelines and protocols are implemented.

While most firms stated that their training programs are computer-based, one bank and two wealth advisory firms stated that instructor-led training was more effective at increasing retention and at conveying the complexity of financial exploitation scenarios. For example, Wells Fargo Advisors launched a training program that uses hypothetical video-based vignettes to guide advisors and client associates through group discussions about elder financial abuse (Long 2014). This training is mandatory for all advisors. Employees are also given instructions on how to *OWN IT*, which involves these five steps:

(1) *Observe*: Notice unusual patterns or changes in a client's behavior. Are there recent changes in the client's health or mental status that may explain the unusual behavior? Is a stranger accompanying the client to meetings, coaching him over the phone, or overly interested in the client's financial affairs?

(2) *Wonder Why:* Question these unusual behaviors. For example, why is the client suddenly requesting a large disbursement of funds? Who is the unknown third party that will receive the funds?

(3) *Negotiate:* Try to convince the client to delay the transaction or to withdrawal a smaller amount until the request can be investigated by the firm.

(4) *Isolate:* Speak with the client privately so that the suspected perpetrator cannot influence the client's responses.

(5) *Tattle:* Report concerns to a supervisor so that the situation can be investigated further and a report made to adult protective services (APS) and/or law enforcement if necessary (Long 2014).

In addition to programs like *OWN IT*, financial service professionals are also being educated about issues related to aging and how declines in cognitive functioning may increase the risk of financial exploitation (Marson 2016; Little & Timmerman 2015). This was identified as a key area of interest among the firms we interviewed. Problems managing money is one of the early areas of cognition to be impaired with age (Marson & Sabatino 2012), and wealth advisors are sometimes the first professionals to notice diminished capacity in their clients. Signs to look for include repeated phone calls to the advisor, inability to recall signing paperwork, forgetting prior conversations, losing track of important documents, trouble understanding financial concepts, and impaired financial judgment such as showing atypical interest in risky investment options (Triebel & Marson 2012). If diminished capacity is suspected, Little and Timmerman (2015) recommend asking the client to bring a trusted family member to the next financial planning meeting and to determine if the client has appointed a durable power of attorney. They also recommend carefully documenting the conversation and following up via a phone call or email.

Training bank employees.

Most Americans do not have personal wealth advisors, but the vast majority have bank accounts (Survey of Consumer Finances 2013). In-person interactions with bank employees are still common among older cohorts. A 2014 Federal Deposit Insurance Corporation (FDIC) survey found that over half of households age 65 and older rely primarily on bank tellers to

access their accounts, compared to less than 20 percent of households younger than age 45 (FDIC 2014). A recent study by AARP found that 70 percent of adults ages 50 and older reported that bank employees recognize them when they visit their local branch, and 32 percent see an employee they know (Gunther 2016). Therefore, educating frontline staff who have high customer touch roles may curb rates of exploitation.

Large depository institutions and payment card retailers are at the forefront of fraud detection using sophisticated algorithms that flag suspicious transfers. The issue is that many signs of financial exploitation—such as unusual signatures on checks or strangers who accompany an older customer to the bank—are not flagged by automated fraud detection systems. In these situations, customer-facing employees are in the best position to notice exploitation and to get others involved. For example, one bank prevented $2.2 million in potential losses through situational training in which frontline employees learned the red flags of exploitation and how to report suspicious activity (Swett & Millstein 2002).

Respondents in the present study stated that developing financial exploitation training programs is costly, particularly for small banks with limited development funds. To address cost issues, financial institution trade organizations are helping their member firms create employee training materials and other media. For example, with support from the Oregon Department of Human Services, Oregon Department of Justice and AARP, the Oregon Bankers' Association developed a training manual and DVD for frontline staff. The Oregon Bank Project (2013) toolkit and training manual outlines warning signs such as sudden changes in beneficiaries or increases in debt, adding third parties to personal accounts, multiple requests to wire money, and unrecognizable handwriting on checks, deposit slips, or loan applications. The toolkit advises staff on what to look for when interacting with customers face-to-face. These warning signs

include: The customer is accompanied to the bank by a ‘new best friend,’ another person speaks on the customer’s behalf without authorization, and the customer is confused and cannot give plausible explanations for unusually large withdrawals. The training manual also features information on relevant laws and response protocols. It is freely accessible online and has been distributed to banks throughout the country. Oregon banks are now the second highest reporters of abuse to APS in the state, even though reporting is not mandatory for financial institutions (Gunther & Neill 2015).

Innovative companies are using ‘gamification’ strategies to make online training more fun and to incent employees to participate. Barclays, one of the United Kingdom’s largest banks with over 10,000 employees, created an interactive web-based training tool called *Community Driving License*. Employees can earn points by taking short quizzes after each module and display their points on the company’s internal social media site. In addition to elder exploitation, the accredited program features modules on how to recognize cognitive impairment and how to make the banking experience more accessible to seniors (Gunther & Neill 2015). Employees can even earn continuing education credits for enrolling in the voluntary program. These incentives have significantly increased participation.

Acknowledging employees for successfully stopping unauthorized transactions improves motivation and reinforces their training. First Financial Bank in Texas instituted a Fraud Busters program to teach 1,200 frontline staff how to recognize and report signs of financial exploitation. Their program is based on three principles—prevention, apprehension, and education. Any employee who successfully spots and reports elder financial exploitation receives public recognition from the CEO and a Fraud Busters pin to wear on her uniform to signify commitment to fighting exploitation. So far, First Financial Bank has saved its customers over $1

million dollars by intercepting potential losses due to fraud and financial abuse (Gunther & Neill 2015).

Bank of American Fork, a small community bank in Utah, selects a full-time employee at each of its retail locations to be the branch's *Age-Friendly Champion*. While all employees receive yearly mandatory training on elder financial exploitation, the Age-Friendly Champions attend quarterly workshops at the firm's headquarters to receive leadership training on issues pertaining to older adults. Dementia, sensory changes, and financial exploitation are all part of the curriculum. These specially trained employees are encouraged to share their knowledge with co-workers and to foster a culture that emphasizes reporting elder financial exploitation to the appropriate authorities (Gunther & Neill 2015). Bank of American Fork stated that the program has been tremendously successful at improving sensitivity to older customers' needs and has generated attention and praise from the media.

Some employee training is virtually free to implement. For example, to raise awareness of elder financial exploitation, Hongkong and Shanghai Banking Corporation (HSBC) screen savers display pictures of older adults alongside information on the warning signs of financial exploitation. These subtle messages remind frontline staff to be mindful of their older customers' vulnerabilities. AARP is planning to create a similar screen saver and distribute it to banks across the country. The screensaver will be customizable so that companies can add their logos and other branding.

Preventing exploitation through community outreach.

Education efforts have moved beyond focusing on frontline staff. Now firms are reaching out directly to their older consumers and family caregivers. Outreach events are typically held at

local senior and community centers, churches, local businesses, libraries, police departments, and civic organizations. Three of the firms we interviewed lead free seminars to distribute fraud prevention materials to clients and their families. For example, Allianz Life partnered with the Better Business Bureau to create the *Safeguarding Our Seniors* volunteer program for Allianz employees and community members. Volunteers go to community and senior organizations to speak about exploitation and financial planning. Collaborating with community groups brings credibility to the banks, builds relationships, and brings media attention to the bank's efforts (Barbic 2015).

Many community outreach and education initiatives are being led by financial institution trade organizations and nonprofits. The American Bankers Association (ABA) Foundation recently launched the *Safe Banking for Seniors* campaign with the goal of helping firms improve their fraud prevention and education program (Barbic 2015). Any bank can participate in the program and download communication resources such as ready-made presentations, handouts on financial exploitation, and 'how-to' guides for hosting educational events. ABA Foundation encourages banks to network with local groups that serve the needs of seniors, like Area Agencies on Aging (AoA) and APS.

ABA also bestows *Community Commitment Awards* to banks that are leading the way in community outreach and age-friendly practices. So far, small and medium sized banks have received the most recognition for their efforts. For example, Bank of the West, which received an Honorable Mention, partners with non-profit organizations to host financial exploitation seminars aimed at low and middle income seniors, and those who live in rural areas. They also support broad consumer awareness initiatives by collaborating with aging advocacy groups to create educational films/projects and to publicize information about scams on social media.

Other banks have received recognition from ABA for their free online toolkits designed to help seniors and their caregivers avoid financial exploitation. Similarly, the AARP Public Policy Institute started BankSafe, an initiative that highlights innovative fraud prevention practices at banks and wealth management firms in the US and abroad. They also assist firms in creating and sharing resources, such as the elder abuse screen saver.

The SEC and FINRA, a self-regulatory organization, also provide resources for consumers and guidance for financial firms. In 2015, FINRA launched the *Securities Helpline for Seniors* (HELPS™) as a resource for securities-related questions and concerns (FINRA 2015). FINRA and SEC also issue investor alerts to inform older consumers about common scams and instructions on how to choose a legitimate financial advisor.

Preventing exploitation through early financial planning.

To remove opportunities for fraud and financial abuse, Lichtenburg (2016) recommends proactive estate planning between financial service professionals and their customers. Some wealth advisors use educational outreach materials described above as conversation starters to get their clients to think about who they wish to appoint as an authorized representative should they be unable to make financial decisions independently. DaDalt and Coughlin (2016) present five financial planning actions that should be addressed sequentially by families and their advisors to support an older person. These are:

(1) Assess current assets

(2) Review income and insurance

(3) Discuss future care preferences

(4) Manage daily expenses

(5) Plan care management

Initiating delicate conversations about aging and cognitive decline was identified as a key challenge by the professionals we interviewed. Older clients may feel threatened when their advisors try to discuss the risks associated with cognitive impairment, particularly those who value autonomy in financial decision-making or who have anxiety about their cognitive abilities and short-term memory. Advisors recommended that these conversations need to occur early in the client-advisor relationship, long before any signs of impairment emerge.

As part of FINRA's *Know Your Customer* rules (SR-FINRA-2011-016), broker-dealers are required to know essential facts about their clients and the authority of each person who acts on behalf of the client. To comply, most firms require their advisors to have a conversation with the client every 3 years (at a minimum). One interview respondent stated that discussions about estate planning could be integrated into these conversations, particularly when the client reaches a particular age or life milestone. This respondent also recommended that firms should institute a policy of 'financial checkups' for clients once they turn 75 or 80. These checkups may help normalize discussions around how and when to transition financial responsibilities to an adult child, a close friend, or another relative.

All the firms we interviewed recognized that it is much harder to intervene when financial abuse is committed by someone close to the client, particularly when this individual already has control over the client's assets. Victims may deny exploitation to protect those they depend on for care and emotional support, and may not want the offender—often an adult child—to be penalized by law enforcement (Enguidanos et al. 2014). Two firms we interviewed recommended that to prevent financial abuse by friends and family, advisors should encourage their clients to name multiple individuals to oversee their finances. Assigning co-trustees and

joint powers of attorney ensures that no single person has full decision-making control and reduces the risk of financial abuse.

The North American Securities Administrators Association (NASAA) is creating power of attorney guidelines and best practices with instructions on what financial advisors should do if an appointed agent is taking advantage of their client. The Consumer Financial Protection Bureau (CFBP) has also issued instructions on how to manage someone else's money. The guides specify the rules and responsibilities of powers of attorney, trustees, and legal guardians. They are publically available at http://www.consumerfinance.gov/managing-someone-elses-money.

A major concern moving forward is that more people are aging without children. Financial advisors are challenged by situations in which a client shows signs of diminished capacity but has no family members or friends with sufficient time, commitment, or skills to act in a fiduciary capacity. One option is to recommend that the client work with a corporate trustee from a bank trust department or an independent trust company (Little & Timmerman 2015). Corporate trustees, though costly, are experts in trust administration and tax considerations. Another option for financial advisors is to contact APS. This should be done if the client is presently being exploited by others and is cognitively impaired, or if he appears to be neglecting his own needs. FINRA (2015) recommends that financial advisors do not act as their client's powers of attorney, trustees, representative payees, or legal guardians, as this gives the advisors too much discretionary control over the client's assets and may lead to abuse.

<u>Financial tools and products that prevent financial exploitation.</u>

To prevent financial abuse of older adults who depend on others for care and support, some companies have introduced products that allow caregivers to help the elder with shopping, transportation, and paying bills, but limit how much total money they can spend. For example, True Link is a debit card designed for families caring for seniors with mild cognitive impairment. The primary caregiver—usually the elder's son or daughter—can set spending limits and restrict the card's functionality to specific venues and retailers, such as the elder's favorite restaurant, a movie theater, or store. The card is meant to preserve the older person's dignity by providing some financial independence, but it blocks others—such as hired personal caregivers—from misusing the elder's funds.

Prepaid debit cards can also be provided to caregivers to purchase needed items, but this system can be exploited by the individual who loads money onto the prepaid cards from the elder's account. Similar to the prepaid card, Barclays now offers a wearable wristband—*bPay*—that acts as a contactless payment card. The user can only spend up to £30 a day at any given vendor. In the future, biometric debit cards that require the accountholder's fingerprint to unlock funds, rather than a pin number, can cut down on the risk of fraud by remote predators (Gunther & Neill 2015).

At nearly every bank, customers can set up recurring automatic transfers from their main account into a joint account they hold with someone else. Caregivers can use the money in this joint account to pay for groceries, medications, utilities, and other services, but they cannot access the rest of the elder's money. Third party account monitoring is another popular online banking service whereby designated individuals have view-only privileges and may receive fraud and/or spending alerts, but cannot withdraw funds or transact business on behalf of the

accountholder. All of these are simple, and largely free interventions that financial institutions are promoting to older customers and their caregivers.

Data-driven strategies to detect financial exploitation.

Spurred by advances in mobile and online payment technology (Heintjes 2014), retail banks have invested in sophisticated fraud management systems to identify suspicious transactions. Some systems rely on user-defined criteria to predict which transactions are fraudulent, whereas others use advanced machine learning algorithms (Joyner 2011). Data might include demographic information about the customer, the amount of money transferred, the location and IP address of the device used, and the patterning of different transactions. More advanced algorithms are now integrating unstructured qualitative data from consumers' social media accounts like Twitter, Yelp, and Facebook. The hope is that by modeling typical patterns of online activity, the financial institution can flag deviations in behavior that signal financial exploitation. These fraud detection algorithms must continuously evolve and incorporate new types of data in order to stay ahead of scam artists. It is important to note that data-driven strategies are used to protect customers of any age against fraud, not just older adults.

When suspicious activity is detected in a customer's account, the banks we interviewed will attempt to contact the customer and alert him or her to potential fraud, usually via an email alert, a letter, or a phone call. Often customers will notice the unauthorized transaction before the bank, and will call customer service directly to make a report. At Wells Fargo and other large banks, complaints are forwarded to an internal claims department for further investigation. The bank may stop the transaction if it is still in progress and reimburse losses depending on the outcome of the claims investigation. Wells Fargo instructs its customer service representatives to use customer contact as an opportunity to educate customers about how to protect themselves

from future fraud attempts. Strategies they recommend are ensuring that all access devices are password protected and that the customer informs the bank in advance about international travel plans and changes in residence.

When accounts are held at different companies, it is challenging for any single institution to model patterns in their customers' financial behaviors and alert them to questionable transactions. A company called EverSafe is attempting to solve this problem by consolidating customers' account information across institutions and by providing daily fraud monitoring. EverSafe analyzes signs such as abnormal cash withdrawals, missing deposits, possible identity theft, and unusual credit bureau activity. Some fraud alerts are based on the common signs of financial exploitation, and others are tailored to the client's personal financial history and spending patterns. The company also helps older clients select a trusted advocate who can help monitor accounts and receive alerts if abnormal activity is detected.

Transaction history data can be used to proactively protect clients from fraud and financial abuse. For example, based on the profiles of elders who were exploited in the past, Barclays applied specific search criteria to identify others in the database who share similar risk factors. One of the parameters they selected was if the customer issued an abnormally high volume of checks in a very short period. Once these high-risk customers were identified, the bank placed a notification on their accounts as an indication to frontline staff to educate the customer on how to reduce risk during any subsequent phone call or visit to the local branch. The UK firm is currently exploring a more direct approach, whereby bank staff contact the customer proactively to discuss fraud risk rather than waiting for the customer to initiate the conversation (Gunther & Neill 2015).

Secondary Interventions.

Federal reporting of elder financial exploitation.

In addition to detecting elder financial exploitation, financial service professionals also receive training in procedures for reporting it. First, all depository institutions and securities firms must submit a Suspicious Activity Report, or *SAR*, to the Treasury Department's Financial Crimes Enforcement Network (FinCEN) within 30 days following an incident. SAR filings help law enforcement agencies identify individuals, groups, and organizations involved in committing fraud, money laundering, and other crimes. In February 2011, a new category—'Elder Financial Exploitation'—was added to the reporting form following advisory notice FIN-2011-A003. The purpose was to encourage institutions to report suspected elder financial abuse and fraud using a standardized term (FinCEN 2013).

FinCEN published a report showing that in the 18 months following the release of the new guidance, there was a 382 percent increase in the number of reports containing the terms 'elder financial abuse' and 'elder financial exploitation' (FinCEN 2013). This increase is shown in Figure 1.

<Insert Figure 1 here>

The reporting trend continues to rise, particularly among banks. In 2015, depository institutions filed over 19,000 elder financial exploitation SARs compared to 10,923 in 2013. As seen in Figure 2, there were only 568 elder financial exploitation SARs filed by securities firms in 2013 compared to 1,763 in 2015. This represents an increase of over 210 percent in just two years.

<Insert Figure 2 here>

Financial abuse by a relative or caregiver was the most common type of elder financial exploitation reported by depository institutions, which, compared to other types of financial

institutions, file the highest number of financial exploitation SARs. Misuse of funds by an appointed power of attorney and the use of coercion to manipulate the client were also frequently cited. Among filers in securities and futures firms, the most common type of activity reported was sweetheart scams, suspicious identification presented, embezzlement, identity theft, and mail fraud. Unusual wire transfers was the most common activity reported by money service businesses, which includes companies like Western Union. Cited activities included wiring funds multiple times a day to different entities in the US or to places outside the country that are classified as 'high-risk,' frequenting multiple money service business locations over a short period of time, and altering the transaction amount to avoid completing a funds transfer record for transactions of $3,000 or more. The most common frauds were bogus lotteries, consumer fraud, and imposter scams, in which a con artist claims to be a friend, relative, or lover in need of immediate funds to cover legal fees or medical bills (FinCEN 2013).

According to FinCEN (2013), the addition of elder financial exploitation as a new SAR filing category has helped protect at-risk seniors. Money service businesses were able to identify and block the majority of suspicious transactions that they filed. FinCEN also claims that the reporting category increased awareness across multiple sectors of the industry, evidenced by how many firms have incorporated elder financial exploitation into their suspicious activity and risk monitoring programs.

Despite some positive evidence that this new category of SAR filings increases awareness, one of the firms we interviewed stated that SARs were ineffective at resolving financial exploitation at the individual case level. These representatives shared their frustration about the apparent inaction by local law enforcement following a report, and stated that this lack of response creates a disincentive to file. Indeed, there has been little indication that regional

SAR Review Teams, comprised of representatives from state and federal law enforcement agencies, have pursued elder financial exploitation cases. One reason is that these reports represent only a small proportion of total SAR filings. Moreover, SARs are considered highly confidential documents. Some local law enforcement agencies must request access to the data from their state coordinators, which may be the state attorney general, state police, or the department of public safety (FinCEN 2012). This process slows investigations and acts as a further disincentive to pursue these challenging cases.

Reporting to Adult Protective Services.

In addition to SARs filings, which are required by firms across all financial service sectors, reporting elder financial abuse to APS is mandatory for financial institutions in 25 states. In other states, such as Iowa and Virginia, financial institution employees are permitted to report abuse to APS but it is not mandatory (Comizio et al. 2015). Laws vary with respect to what types of financial professionals are included under the law—bankers, accountants, broker-dealers, etc.—and who at a company must report—a director or officer of the institution or any affiliated employee. Table 1 presents which states have mandatory reporting laws for financial institutions and who at the institution must make the report.

<Insert Table 1 here>

At the majority of firms we interviewed, the policy is for customer-facing employees and financial advisors to relay their suspicions of financial exploitation to a supervisor or a manager. The supervisor can escalate the case to an internal legal team that decides whether to report it to APS and/or law enforcement. Wells Fargo Advisors created an Elder Strategy Group, a central intake office comprised of lawyers and paralegals who specialize in elder financial exploitation.

The team receives reports from advisors and client associates located anywhere in the country, investigates the allegations internally, and contacts the local APS office where the client resides if the allegations need to be investigated further and if the client needs protection. Out of 1,860 incoming matters between January through December 2015, 818 were reported to APS or law enforcement. Approximately 32 percent of these cases involved suspected abuse by family members, 23 percent involved exploitation by third parties—caregivers, neighbors, and friends—and 10 percent were scams by strangers (Long 2015). Although not all states require elder abuse reporting by financial institutions, Wells Fargo Advisors considers itself a mandated reporter across all locations and may contact APS regardless of any particular states' requirements (Long 2014).

Financial institutions initially opposed mandatory reporting laws because of liability concerns, fear of jeopardizing customer trust, and lack of confidence that their reports would be addressed promptly and effectively by APS (Swett & Millstein 2002). Some interview respondents shared an attitude that reporting could potentially increase the client's risk of harm by the perpetrator if he becomes aware of APS involvement, and that even if APS can help, the agency is too understaffed and overwhelmed by the high volume of cases to help. As a result, some of the firms we interviewed prefer to resolve the less serious cases internally, such as by helping recover lost assets and getting other family members involved; however, they recognize the importance of involving social services if the client is not safe.

Although many concerns were raised about the efficacy of mandatory reporting, it is clear that these laws have increased the total number of cases that are seen by APS, meaning that more crimes are being investigated. For example, after mandatory reporting laws were revised to include financial institutions in California, reports from financial institutions jumped from 127

cases in 2006, to 940 cases in 2007, representing a 640 percent increase (Navarro et al. 2009). It is unclear whether laws that mandate reporting are necessary and sufficient to motivate financial professionals to report. According to one interview respondent, states such as Massachusetts and Oregon have been successful at increasing reports to APS despite not having laws that make it mandatory. To help address some of the current limitations in elder abuse response and to increase visibility around the issue, the Securities Industry and Financial Markets Association (SIFMA), a trade organization for financial advisors, advocates increasing APS funding (SIFMA 2016).

Working with law enforcement.

When financial exploitation has occurred, the key priorities for financial institutions and victim advocates are to protect the older person and to try to recover assets. Other priorities are ensuring that the perpetrator is apprehended and that appropriate legal and criminal justice outcomes are pursued. These solutions generally require law enforcement and APS involvement. Contacting these agencies can also prevent re-victimization and ensure the client's assets are protected. We interviewed a financial crimes detective who shared a story about a local branch manager who called police immediately when an elderly customer requested an unusually large withdrawal and was shadowed by a stranger during a visit to her bank. A deputy responded immediately and arrested the suspect in the parking lot. The scam artist, who was also attempting to fleece other seniors in the area, may have continued on with this scheme if law enforcement had not been contacted.

Criminal prosecution of those who exploit vulnerable adults is only possible through cooperation and information sharing with law enforcement. The financial crimes detective stated that banks and financial advisors should have contacts at their local police or sheriff's stations to

advise them on what to do and to facilitate investigations of fraud and financial abuse. To comply with investigations, firms can help law enforcement by promptly releasing client financial records and other supporting evidence, such as ATM camera and CCTV footage that may help identify the perpetrator. The detective stated that although banks have improved communication with police on issues related to elder fraud and financial abuse, more collaboration and relationship building is needed, perhaps by creating opportunities for cross training.

The Regulatory Puzzle.

Current regulations both challenge and facilitate client protection efforts by financial service firms. If a client is cognitively intact, financial professionals must execute his orders and protect his privacy, even if they believe the client is making a poor financial decision. Interfering with a transaction by placing a hold on the account or by alerting family members to potential exploitation may result in lawsuits from the client and/or penalties from the regulatory bodies that oversee the financial service industry. Yet there is equal pressure from these regulators to protect clients from fraud and financial abuse. The firms we interviewed stated that the contradictory pressures from regulators places them in legal limbo, particularly when confronted with complex or ambiguous financial exploitation scenarios.

According to our interviews, firms wanted to do more to protect older clients, and regulators agreed that more actions are necessary, but the complicated patchwork of state and federal oversight, shown in Figure 3, makes it difficult to have a consistent response to elder financial exploitation.

<Insert Figure 3 here>

For example, depending on their designation and certification, financial planners are governed by different entities and different laws (US Government Accountability Office 2011). Registered investment advisors are regulated either by their state securities departments and/or by the SEC, depending on the size of the firm. FINRA, which is an independent self-regulatory membership-based organization (SRO), is empowered by the SEC to oversee broker-dealers, or individuals that can buy and sell securities. Although banks and financial advisors have similar rules governing customer privacy and reporting elder financial exploitation, banks are regulated by prudential regulators such as the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve Board System, the Office of the Comptroller of the Currency (OCC), and also by the Consumer Financial Protection Bureau (CFPB), an enforcement agency.

Privacy Concerns.

The primary concern among interview respondents was violating regulations intended to protect customer privacy. The Gramm-Leach-Bliley Act (GLBA § 504(a) (1)), passed in 1999, requires financial institutions to inform clients about their privacy policies, describe the conditions under which they may disclose nonpublic personally identifiable financial information to third parties, and provide a way for clients to opt out of information sharing. Without the client's consent, financial institutions cannot contact the client's next of kin if they suspect cognitive impairment or exploitation. However, a close inspection of the GLBA shows that there are important exceptions to these privacy rules (Hughes 2003). First, notification and opt-out requirements do not apply in situations where the firms act to 'protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability' (G-L-B Act § 248.15(2)(ii)). Second, client information can be shared with local law enforcement agencies and federal regulators, and it can be shared to comply with 'a properly authorized civil, criminal, or

regulatory investigation, or subpoena or summons by federal, state, or local authorities' (G-L-B Act § 248.15(7) (ii)). Therefore, financial institutions and their employees have immunity from civil liability when reporting known or suspected financial exploitation, even if the allegations are ultimately not substantiated. This protection includes disclosing information to comply with voluntary or mandatory reporting laws and to file suspicious activity reports with FinCEN (Office of the Comptroller of the Currency 2013).

There are also statutory and case laws that protect personal financial information, but most have exceptions for disclosing financial records to APS and law enforcement. Other than one state, South Dakota, APS laws provide immunity from civil and criminal liability to *any person* who reports elder financial abuse as long as they reported in good faith. A problem is that these laws do not specify whether 'any person' applies only to the individual employee or to the financial service firm as an entity.

Similar to the GLBA, the Right to Financial Privacy Act of 1978 ('RFPA') protects confidentiality of personal financial records. A customer must be given prior notice and an opportunity to challenge the federal government's action in court before the government can obtain his or her private financial information from the firm; however, the RFPA applies only to the federal government, not to state and local agencies such as APS and police departments. These agencies can obtain customer financial records for investigate purposes. For example, if a bank teller in California suspects that a family member is manipulating an older client with dementia to withdrawal funds from his savings account, the teller may report her concerns to a supervisor. The supervisor must file a SAR, contact APS, and can share the client's financial records with law enforcement when requested. None of these actions violate the provisions of GLBA or RFPA.

Part of what prompted financial privacy laws was a concern among consumers that their personal information was being sold to marketers and released to federal agencies to investigate crimes related to tax evasion. While consumers may have fewer unwanted solicitations and less surveillance by the federal government as a result of these regulations, the unintended effect is that well-intended financial service professionals feel they have less authority to protect their clients against fraud and financial abuse.

Rule changes and safe harbor protections

Wealth advisory firms stated that universal standards and safe harbor protections would enable them to do more to protect clients without fear of incurring liability. Many are taking a proactive approach and asking new clients to specify one or more 'emergency contacts' when they first open an account with the firm. Wells Fargo Advisors requests that its clients complete an 'ICE' form (In Case of Emergency) that authorizes them to contact these designated individuals if the financial advisor believes the client is at risk of financial exploitation. Some emergency contact forms are modeled after advanced healthcare directives—they provide flexibility by allowing the client to specify what personal information can be shared with a specified contact and under what conditions. Unlike a power of attorney, the emergency contact form does not authorize the specified individual(s) to transact business on behalf of the client, only to receive information related to the financial advisor's concerns.

Encouraging every new client to name one or more emergency contacts will likely become a standard practice in years to come, but the forms have not yet been widely implemented and firms will be slow to collect this information from their existing clients. Financial institutions grapple with situations in which a vulnerable client failed to provide authorization in advance, and situations in which the client has no trusted friends or family

members to name as his emergency contacts. Financial advisors also fear that by delaying potentially fraudulent transactions, they may face liability for failing to execute the client's orders.

New legislation is being proposed to address these fears. On August 23rd 2015, Missouri became the first state to pass landmark legislation, the Senior Savings Protection Act (MO Senate Bill 244/House Bill 636), that allows broker-dealers to breach privacy laws without being subject to civil liability suits as long as they have reason to suspect a client is a being financially exploited. A qualified individual at the firm (a supervisor or compliance officer) is permitted to notify the client's legal representative or an immediate family member, such as a spouse, child, or sibling. The Act also allows financial advisors to hold a questionable disbursement for up to 10 business days without penalty and report elder financial exploitation to the Department of Health and Senior Services and the Missouri Securities Commission. Delaware and Washington have similar laws that allow financial advisors regulated by the state to refuse clients' orders if they suspect financial exploitation. This provides a short window for APS and/or family members to intervene before the client's money vanishes.

With support from their trade organizations, investment advisors from around the country have encouraged NASAA and FINRA to follow Missouri's lead and pass similar laws at the state and federal levels, so that more broker-dealers and registered investment advisors are covered. Both organizations have recently issued rule proposals that give advisors safe harbor protections from civil and administrative liability for intervening in cases of fraud and financial abuse, but there are important differences between the proposals. NASAA's Model Act, issued in September 2015, permits firms to reach out to others if exploitation is suspected, but only if the client (age 60 and older) previously named these individuals as his or her emergency contacts. It

does not provide legal protection if the advisor did not obtain authorization in advance. As a Model Act, NASAA's proposal would need to be enacted by individual states before it becomes law.

FINRA's rule proposals (amendments to rules 4512 and 2165) require that firms make *reasonable efforts* to proactively obtain contact information for a trusted person when an account is opened or in the course of updating account information, but if no trusted person is listed on the account, firms are permitted to breach privacy rules and contact an immediate family member of their choosing (FINRA Regulatory Notice 15-37 2015). NASAA's proposal permits the firm to place a hold on the disbursement of funds or securities for up to ten days if they suspect exploitation *or* have concerns about diminished financial capacity, whereas FINRA's proposal allows a 15-day hold but only in response to suspected exploitation. Once the hold is in place, the firm must immediately review the facts and circumstances that led them to believe that exploitation is occurring, has been attempted, or will be attempted. NASAA's proposal mandates that all firms report to APS, but FINRA's proposal leaves APS reporting requirements up to the states. Comments on FINRA's rule proposal expired on November 30th 2015. Because State Securities Regulators oversee more designations of financial planners than FINRA, which is a membership-based SRO, adoption of NASAA's proposal may have greater impact across the industry. As these new rules offer more flexibility and safe harbor protection, the regulators we interviewed stated that they do not anticipate significant pushback from firms in the passage of the laws.

Regulation S-ID: Preventing identity theft.

In April 2013, CFTC and SEC issued a joint rule, Regulation S-ID under the Dodd-Frank Act, which is designed to protect consumers from identity theft. This rule also protects

individuals from fraud and financial abuse because it requires broker-dealers, investment companies, and investment advisors to establish and maintain programs for verifying investors' identities and for detecting the red flags of identity theft. Many of these signs overlap with financial exploitation. The rule requires that firms monitor accounts for fraudulent activity, respond when altered or forged documents are presented to advisors, and determine the validity of address change requests. Firms must also have procedures for contacting the customer and/or law enforcement to report identity theft, and escalation procedures to refer the case to investigators. Institutions must train staff in implementing their identity theft procedures and conduct ongoing assessments of the program's effectiveness. Firms are permitted to close existing accounts and can refuse to open new accounts if identity theft is suspected. Thus, Regulation S-ID makes it harder for scam artists and opportunistic family members to gain access to an older client's accounts and to make unauthorized withdrawals.

Regulation E: Protecting electronic fund transfers.

Most cases of fraud and identity theft are perpetrated through electronic channels using an access device, such as when a caregiver steals an elder's debit card and pin number to withdrawal funds. The Electronic Fund Transfer Act, or Regulation E (12 CFR 205), protects consumers from losses associated with unauthorized ATM withdrawals, point-of-sale terminal transactions in stores, and preauthorized transfers to or from an account such as direct deposit of social security payments or automatic bill pay. When a fraudulent transaction occurs, losses to the accountholder are limited to $50 as long as the customer informs his bank within two business days after learning of the loss. Customer liability increases to up to $500 (or up to the value of the stolen funds) after those two days. If the customer fails to notify the bank of the

unauthorized charges after 60 days the institution is no longer responsible for covering any portion of the loss and the customer is fully liable.

Regulation E only protects consumers if the transaction was unauthorized. If an elder willingly gives his debit card and pin number to his caregiver to buy him groceries, and the caregiver drains his bank account, Regulation E does not apply. Regulation E also does not cover transfers of securities purchased or sold through broker-dealers, wire transfers between financial institutions, or counterfeit checks, meaning that other mechanisms through which fraud and financial abuse are perpetrated are not covered under the law. Furthermore, older customers with cognitive impairments may be unaware that they were victimized and may fail to report losses to their bank within the 60-day period. These vulnerable consumers face the risk of losing their entire savings to scams and fraud committed electronically.

Present challenges

There are a number of problems that still need to be addressed to improve the industry's response to elder financial exploitation. One wealth advisory firm stated that the three barriers to improving detection and response to financial exploitation are: (1) the high cost of implementing changes to policies and procedures, (2) restrictive legislation, and (3) insufficient personnel. The securities regulators we interviewed expressed concern that firms were not doing enough to protect their clients, but worried that allowing them to delay transactions and break privacy rules would give the financial industry significantly more power. Their primary concern was that elder financial exploitation is hard to diagnose with absolute certainty. Without clear guidelines that specify exactly when firms can intercede, they may infringe on their clients' liberty to make independent financial choices; or, firms may unintentionally disclose information to a perpetrator if he or she is named as the client's emergency contact. Interview respondents recommended

more standardized rules and guidance to help firms decide what to do when faced with ambiguous situations.

We found that there is considerable variability in how firms respond to elder financial exploitation, even within the same company. Regulators stated that although banks have many of the same SAR obligations and privacy rules as broker-dealers, their practices for protecting older customers lag behind, likely because their services are transaction-based rather than relationship-based. While this lack of consistency is partially due to differences in state mandatory reporting laws and which regulatory bodies oversee the various sectors of the financial service industry, companies would be better equipped to combat financial exploitation if they shared resources across departments and institutions. This would also help save on program development costs.

There are considerable barriers to resolving elder financial exploitation cases. According to our interview with a financial fraud detective, the policy of internally escalating cases of suspected financial exploitation to compliance officers within the firm makes it difficult for local investigators to respond quickly. Law enforcement needs to be informed of potential criminal activity immediately to apprehend perpetrators, and APS workers also need to be notified to ensure the elder's safety. When firms are slow to report, perpetrators have more time to spend the elder's money and to cover their tracks.

Another challenge for detectives is obtaining client financial records to support criminal cases against perpetrators, even in cases where firms reported directly to police. In 2007, FinCEN issued guidance on the legality of disclosing private financial information to investigatory agencies (FinCEN 2007). The guidance states that when an institution files a SAR, it must retain and provide all documentation supporting the SAR to law enforcement and/or to appropriate supervisory agencies upon request. This disclosure is protected by safe harbor

provisions and no legal process is required, yet some firms require law enforcement to fax them a warrant from a judge before releasing information. Others require a warrant to be delivered in person. The inconsistency in procedures and additional hurdles to obtaining evidence creates another barrier to law enforcement officers who already have minimal training in how to investigate complex financial crimes. As a result, perpetrators rarely face prosecution for elder financial exploitation (Navarro et al. 2014).

Representatives at the firms we interviewed agreed that collaborative partnerships with local law enforcement and APS agencies are needed. They suggested that law enforcement provide the firm with regular updates on the progress of fraud investigations and the outcomes of the case. However, the laws are such that detectives and APS workers are not allowed to share information about an open case which could potentially compromise their investigation (Swett & Millstein 2002). This lack of communication between financial firms and local investigators may protect the privacy of those involved, but also creates a disincentive to report as some employees feel their concerns are ignored.

One solution to this fragmentation in communication is encouraging representatives at each firm to participate in local multidisciplinary teams that help coordinate inter-agency response to elder financial exploitation. Examples include Elder Abuse Forensic Centers and Fiduciary Abuse Specialist Teams. Member agencies generally include local law enforcement, APS, district attorneys, victim advocates, social services, legal services, and physical and mental health providers. The goals of these partnerships are to ensure the safety of the client, collect comprehensive and accurate information useful for legal proceedings (e.g., prosecutions and/or guardianship/conservatorship), and to secure the client's property and assets (Navarro et al.

2015). Though confidentiality provisions differ across states, most laws permit team members to share information with each other without violating privacy rules.

Research shows that collaboration among stakeholders increases the odds of criminal prosecution of offenders and conservatorship of vulnerable adults who are victims of financial exploitation (Navarro et al. 2013; Gassoumis et al. 2015). Elder abuse multidisciplinary teams would benefit from participation by financial service professionals who can provide expertise in forensic accounting and build a bridge between the financial service industry, the adult protection system, and the criminal justice system. The firm would benefit from greater community involvement, networking opportunities, and an improved understanding of inter-agency response to elder financial exploitation.

The Future

Proactive strategies that prevent financial exploitation can be a powerful business differentiator in a crowded financial services marketplace. Large firms have the capital to invest in training and consumer education programs to combat fraud and financial abuse, yet they also have more rigid protocols. Community banks are more nimble and can adapt their protocols based on what services they provide, the regions they operate in, and the age of their clients, but they also have smaller budgets to invest in these initiatives.

Financial service trade organizations are supporting member firms by developing training resources and consumer education materials. SIFMA launched an online Senior Investor Protection Resource Center where member firms can downloaded free resources. Trade organizations have also established partnerships with adult protection agencies, senior advocacy

groups, and other professionals that work with vulnerable adults. ABA Foundation teamed up with AARP to launch the Safe Banking for Seniors campaign, and NASAA partnered with the National Adult Protective Services Association and physician groups to increase awareness.

Aging and consumer advocacy groups can put pressure on regulators to improve and clarify laws so that banks and wealth advisory firms are operating under standardized regulations. Consumers can also motivate the industry to do better by patronizing firms that offer more age-friendly services and demonstrate a commitment to protecting older adults. An AARP survey reported that over 80 percent of adults age 50 and older prefer to establish accounts at banks that offer services to protect them against financial exploitation, such as extra account monitoring, phone calls to warn about suspicious activity, and having highly trained bank staff (Gunther 2016).

There is tremendous opportunity for the financial service industry to engage with researchers to better understand elder financial exploitation, particularly in mapping patterns in customers' spending and saving behavior to proactively identify those most at risk, the mechanisms through which money changes hands, and possible touch points for educating customers on avoiding fraud and financial abuse. To our knowledge, there have been no studies evaluating the efficacy of different training programs to determine whether they increase detection of financial exploitation and reporting. There is also scarce data on the total value of assets that have been protected or recovered using different prevention strategies, and whether customers are satisfied with their firm's response. Companies should turn to research before investing time and money on potentially ineffective programs.

Research in behavioral economics and decision neuroscience could also inform the industry about how age-related changes in decision-making increase the risk of exploitation.

Most decision research is conducted in laboratory settings where participants are given hypothetical endowments of funds and instructed to make purchase decisions among a fixed set of options. These findings do not necessarily generalize to applied situations in which consumers use their own money in various contexts. This represents an enormous gap in the literature and highlights a need to develop protocols for how researchers can work with the private sector's data and clients without violating privacy laws or jeopardizing data security.

Conclusion

Financial services are changing rapidly with advances in technology. The personal relationships that firms have with their clients and customers will become less common as millennials eventually replace baby boomers as the primary users of financial services. New technologies are shaping how often and in what capacity consumers interact with bank staff and financial advisors. While 89 percent of Americans age 50 and older visit their bank in person (Gunther 2016), younger customers are relying more and more on online banking for making transactions and viewing account balances (TD Bank 2014). Contemporary services include mobile apps for instantly transferring funds person-to-person, credit card readers that plug into phones, and 'robo-advisors' for automatically selecting and managing diversified investment portfolios instead of hiring personal financial advisors.

New access devices and increased automation will not stop fraud and financial abuse. These services may perhaps make the problem worse. How will emerging technologies be engineered to detect diminished financial capacity, undue influence, and other subtle signs of exploitation as younger generations grow older and more vulnerable? The financial service

industry must mobilize to protect the older clients of today, and invest in solutions that protect future financial services customers.

Acknowledgements:

The authors would like to acknowledge the interview respondents for their time and dedication to preventing elder financial exploitation within their organizations. We are especially grateful to Lori Stiegel, Liz Loewy and many others for their contributions, particularly their knowledge of state mandatory reporting laws and federal regulation surrounding this important issue. A special thank you to Ronald Long, Lori Schock, Christine Kieffer, Gerri Walsh, Armand Abhari, Katie Libbe, Surya Kolluri, and Allyson Young for facilitating interviews with industry representatives, regulators, and law enforcement officers. We are also grateful to Bill Stutts and Ken Scott for their expert knowledge of financial service industry regulation. Many thanks to Gary Mottola at the FINRA Investor Education Foundation for reviewing the manuscript and to Jilenne Gunther at AARP Public Policy Institute for connecting us to smaller financial institutions and other professionals who helped inform this chapter.

References

Acierno, R., M. A. Hernandez, A. B. Amstadter, H. S. Resnick, K. Steve, W. Muzzy and D. G. Kilpatrick (2010). 'Prevalence and Correlates of Emotional, Physical, Sexual, and Financial Abuse and Potential Neglect in the United States: The National Elder Mistreatment Study,' *American Journal of Public Health,* 100: 292–297.

Anderson, K. B. (2013). *Consumer fraud in the United States, 2011: The Third FTC Survey.* Washington, DC: Federal Trade Commission.

Barbic, K. (2016). 'Safe Banking, Savvy Seniors,' *American Bankers Association Banking Journal,* 108(1): 36–38.

Barclays (2016). 'bPay,' *Barclaycard* [website], <https://www.bpay.co.uk/home>

Bonnie, R. and R. Wallace (2003). *Elder Mistreatment: Abuse, Neglect, and Exploitation in an Aging America*. Washington, DC: National Academies Press.

Button, M., J. Gee, C. Lewis, and J. Tapley (2010). *The Human Cost of Fraud: A Vox Populi.* Centre for Counter Fraud Studies & MacIntyre Hudson. http://www.port.ac.uk/departments/academic/icjs/centreforcounterfraudstudies/documents/filetodownload,116542,en.pdf

Certified Financial Planner (CFP) Board of Standards. (2012). 'Senior Financial Exploitation Study,' https://www.cfp.net/docs/news-events---supporting-documents/senior-americans-financial-exploitation-survey.pdf?sfvrsn=0

Comizo, G., A. Kowalski, and L. Bain (2015). 'Elder Financial Abuse on the Rise: What Financial Institutions Can Do to Address Increasing Regulatory Scrutiny Designed to Protect At-Risk Customers,' Paul Hastings LLC. http://www.paulhastings.com/docs/default-source/PDFs/stay-current-elder-financial-abuse-on-the-rise-what-financial-institutions-can-do-to-address-increasing-regulatory-scrutiny.pdf

Conrad, K. J., M. Iris, J. W. Ridings, K. P. Fairman, A. Rosen, and K. H. Wilber (2011). 'Conceptual Model and Map of Financial Exploitation of Older Adults,' *Journal of Elder Abuse & Neglect*, 23(4): 304–325.

Consumer Financial Protection Bureau (CFPB) (2015). 'Guides for managing someone else's money,' *CFBB* [website], <http://www.consumerfinance.gov/managing-someone-elses-money>

Cordray, R. (2015). 'Press Release: Prepared Remarks of CFPB Director Richard Cordray at the White House Conference on Aging Regional Forum,' Washington, DC: April 27.

DaDalt, O. and J. F. Coughlin. (2016). 'Managing Financial Well-Being in the Shadow of Alzheimer's Disease,' *Public Policy & Aging Report*, 26(1): 36-38.

Deem, D. (2000). 'Notes from the Field: Observations in Working with the Forgotten Victims of Personal Financial Crimes,' *Journal of Elder Abuse and Neglect*, 12(2): 33-48.

Deevy, M. and M. Beals (2013). *The scope of the problem: An Overview of Fraud Prevalence Measurement*. Stanford, CA: Financial Fraud Research Center.

http://fraudresearchcenter.org/wp-content/uploads/2013/11/Scope-of-the-Problem-FINAL_corrected2.pdf

Enguidanos, S., M. DeLiema, I. Aguilar, J. Lambrinos, and K. H. Wilber (2014). 'Multicultural Voices: Attitudes of Older Adults in the United States about Elder Abuse,' *Ageing & Society,* 34: 877-903.

Federal Deposit Insurance Corporation (FDIC) (2014). *2013 FDIC National Survey of Unbanked and Underbanked Households*. Washington, DC: FDIC. https://www.fdic.gov/householdsurvey/2013report.pdf

Heintjes, T. (2014). 'How We Pay: Results from the Federal Reserve's Latest Payments Study,' *EconSouth*: Federal Reserve Bank of Atlanta, January-April 2014: 21-24.

Hughes, S. L. (2003). 'Can Bank Tellers Tell? Legal Issues Relating to Banks Reporting Financial Abuse of the Elderly,' American Bar Association, Commission on Law and Aging. http://www.ncea.aoa.gov/resources/publication/docs/bank_reporting_long_final_52703.pdf

Holtfreter, K., M. D. Reisig, D. P. Mears, & S. E. Wolfe (2014). 'Financial Exploitation in the Elderly Consumer Context,' Final report to the U.S. Department of Justice. Document No.: 245388.

Financial Crimes Enforcement Network (FinCEN) (2007). 'Guidance: Suspicious Activity Report Supporting Documentation,' FIN-2007-G003, Department of the Treasury Financial Crimes Enforcement Network. Issued June 13, 2007.

Financial Crimes Enforcement Network (FinCEN) (2012). 'The SAR Activity Review: Trends, Tips & Issues,' *BSA Advisory Group,* Issue 22. https://www.fincen.gov/news_room/rp/files/sar_tti_22.pdf

Financial Crimes Enforcement Network (FinCEN) (2013). 'The SAR Activity Review: Trends, Tips & Issues,' *BSA Advisory Group,* Issue 23. https://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf

Financial Industry Regulatory Authority (FINRA) (2015). *Report on the FINRA Securities Helpline for Seniors.* Washington, DC: FINRA. http://www.finra.org/sites/default/files/Securities_Helpline_for_Seniors_Report.pdf

Financial Industry Regulatory Authority (FINRA) (2011). '2090 Know Your Customer SR-FINRA-2011-016,' FINRA Manual. Effective July 9, 2012.

Financial Industry Regulatory Authority (FINRA) (2015). *Regulatory notice 15-37: Financial exploitation of seniors and other vulnerable adults.* Washington, DC: FINRA http://www.finra.org/industry/notices/15-37

FINRA Investor Education Foundation (2015). *The Non-Traditional Costs of Financial Fraud: Report of Survey Findings*. Washington, DC: Applied Research and Consulting and FINRA Foundation. http://www.finrafoundation.org/web/groups/sai/@sai/documents/sai_original_content/p602454.pdf

Gassoumis, Z. D., A. E. Navarro, and K. H. Wilber (2014). 'Protecting Victims of Elder Financial Exploitation: The Role of an Elder Abuse Forensic Center in Referring Victims for Conservatorship,' *Aging & Mental Health*, 19(9): 1-9.

Gunther, J. (2016). 'BankSafe: A Comprehensive Approach to Better Serving and Protecting Consumers,' Washington, DC: AARP Public Policy Institute.

Gunther, J. and R. Neill. (2015). *Inspiring Case Examples: Age-Friendly Banking.* Washington, DC: AARP Public Policy Institute.

Jackson, S. L. (2015). 'The Vexing Problem of Defining Financial Exploitation,' *Journal of Financial Crime*, 22(1): 63-78.

Joyner, E. (2011). 'Detecting and Preventing Fraud in Financial Institutions,' Cary, NC: SAS Global Forum, Paper 029-2011.

Lichtenberg, P. A. (2016). 'New Approaches to Preventing Financial Exploitation: A Focus on the Banks.' *Public Policy & Aging Report*, 26(1): 15–17.

Little, D. and S. Timmerman. (2015). 'Financial Incapacity and the Aging Baby Boomers: What is the Role of Financial Service Professionals?' Faculty Publications: Paper 317.

Lock, S. L. (2016). 'Age-Friendly Banking: How Can We Help Get it Right before Things Go Wrong,' *Public Policy & Aging Report*, 26(1): 18–22.

Long, R. C. (2014). 'Elder Financial Abuse,' *Elder Abuse and Its Prevention: Forum on Global Violence Prevention*. Washington, DC: National Academies Press.

Long, R. C. (2014). 'Number of ECI Cases Opened by Type, January 2015-December 2015,' [Presentation], Wells Fargo Advisors.

Long, R. C. (2016). ‘Wells Fargo Advisors’ Elder Client Initiatives: A Review of the First Year.’ *Public Policy & Aging Report*, 26(1): 34–35.

Marson, D. C. (2016). ‘Commentary: A Role for Neuroscience in Preventing Financial Elder Abuse,’ *Public Policy & Aging Report*, 26(1): 12-14.

Marson, D. C. and C. Sabatino (2012). ‘Financial capacity in an aging society,’ *Generations*, 36(2): 6-11.

MetLife Mature Market Institute. (2009). *Broken trust: Elders, family, and finances.* New York, NY: Metropolitan Life Insurance Company. https://www.metlife.com/mmi/research/broken-trust-elder-abuse.html#findings

National Center on Elder Abuse (NCEA) (1998). *The national elder abuse incidence study*. Washington, DC: NCEA. http://aoa.gov/AoA_Programs/Elder_Rights/Elder_Abuse/docs/ABuseReport_Full.pdf

National Council on Aging (NCOA) (2015). ‘Top 10 Financial Scams Targeting Seniors’ [website] < https://www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors/>

Navarro, A. E., Z. Gassoumis, and K. H. Wilber, (2009). ‘Press Release: Los Angeles County Adult Protective Services: Trends in financial abuse reports 2005-2008,’ Los Angeles, CA: University of Southern California.

Navarro, A. E., Z. D. Gassoumis, and K. H. Wilber (2013). 'Holding Abusers Accountable: An Elder Abuse Forensic Center Increases Criminal Prosecution of Financial Exploitation,' *The Gerontologist*, 53(2): 303-312.

Navarro, A. E., J. Wysong, M. DeLiema, E. L. Schwartz, M. B. Nichol, and K. H. Wilber (2015). 'Inside the Black Box: The Case Review Process of an Elder Abuse Forensic Center,' *The Gerontologist* [advanced online access].

Office of the Comptroller of the Currency (OCC) (2013). 'Interagency Guidance,' OCC Bulletin, October 4. http://www.occ.treas.gov/news-issuances/bulletins/2013/bulletin-2013-21.html

Oregon Banker's Association (2013). 'Preventing Elder Financial Exploitation: How Banks Can Help,' Elder Financial Exploitation Prevention Project. Oregon Department of Justice, Oregon Department of Human Services Office of Adult Abuse Prevention and Investigations.

Pak, K. and D. Shadel (2011). 'AARP Foundation National Fraud Victimization Study.' Washington, DC: AARP Foundation. http://assets.aarp.org/rgcenter/econ/fraud-victims-11.pdf

Pew Research Center (2014). 'Chapter 4. Population Change in the U.S. and the World from 1950 to 2050,' Washington, DC: Pew Research Center. http://www.pewglobal.org/2014/01/30/chapter-4-population-change-in-the-u-s-and-the-world-from-1950-to-2050/

Securities Industry and Financial Markets Association (SIFMA) (2016). 'Senior Investor Protection Resource Center,' *SIFMA*, [website] <http://www.sifma.org/issues/savings-and-retirement/senior-investor-protection/overview/>

Senior Savings Protection Act (2015). 'Missouri Senate Bill 244/House Bill 636,' Enacted August 23, 2015.

Swett, L. and R. Millstein. (2002). 'The Philadelphia APS Bank Reporting and Loss Prevention Program,' Philadelphia, PA: National Adult Protective Services Association http://www.napsa-now.org/wp-content/uploads/2012/06/Phila-Project-Report-FINAL.pdf

Survey of Consumer Finances (2013). *Federal Reserve Board.* [Data file]. <http://www.federalreserve.gov/econresdata/scf/scfindex.htm>

TD Bank (2014). 'The Millennial: Financial Behaviors and Needs' *Angus Reid Public Opinion*. https://mediaroom.tdbank.com/surveys?item=34208

Titus, R. M., F. Heinzelmann, and J. M. Boyle (1995). 'Victimization of Persons by Fraud,' *Crime & Delinquency,* 45: 54-72.

Triebel, K. L. and D. C. Marson (2012). 'The Warning Signs of Diminished Financial Capacity in Older Adults,' *Generations,* 36(2): 39–45.

US Government Accountability Office (GAO) (2011). *Regulatory Coverage Generally Exists for Financial Planners, but Consumer Protection Issues Remain.* GAO-11-235. Washington, DC: GAO.

US Government Publishing Office (1978). ‘Regulation E: Electronic Fund Transfers: 12 CFR 205,’ Enacted by the 95th United States Congress.

US Government Publishing Office (1978). ‘Right to Financial Privacy Act: 12 U.S. Code Chapter 35 § 3401,’ Enacted by the 95th US Congress.

US Government Publishing Office (1999). ‘Gramm-Leach-Bliley Act Public Law 106-102,’ Enacted November 12, 1999.

Table 1. Mandatory reporting laws for financial service institutions and their employees by state (2015)

States without mandatory reporting	States with mandatory reporting (any employee)	States with mandatory reporting (financial institution)	States with voluntary reporting laws
Alabama	Arizona	District of Columbia	Iowa
Alaska	Arkansas	Hawaii	Missouri
Connecticut	California	Kansas	Nevada
Idaho	Colorado	Maryland	New Jersey
Illinois	Delaware	Washington[a]	Vermont
Maine	Florida		Virginia
Massachusetts	Georgia		
Michigan	Indiana		
Minnesota	Kentucky		
Montana	Louisiana		
Nebraska	Mississippi		
New York	New Hampshire		
North Dakota	New Mexico		
Ohio	North Carolina		
Oregon	Oklahoma		
Pennsylvania	Rhode Island		
South Dakota	South Carolina		
West Virginia	Tennessee		
Wisconsin	Texas		
	Utah		
	Wyoming		

Notes:

[a] A financial institution must report when it refuses to disburse funds based on a reasonable

belief that financial exploitation of a vulnerable adult may have occurred, may have been attempted, or is being attempted.

Source: National Adult Protective Services Association Elder Financial Exploitation Advisory Board and EverSafe (2015, October). Nationwide Survey of Mandatory Reporting Requirements for Elderly and/or Vulnerable Persons.

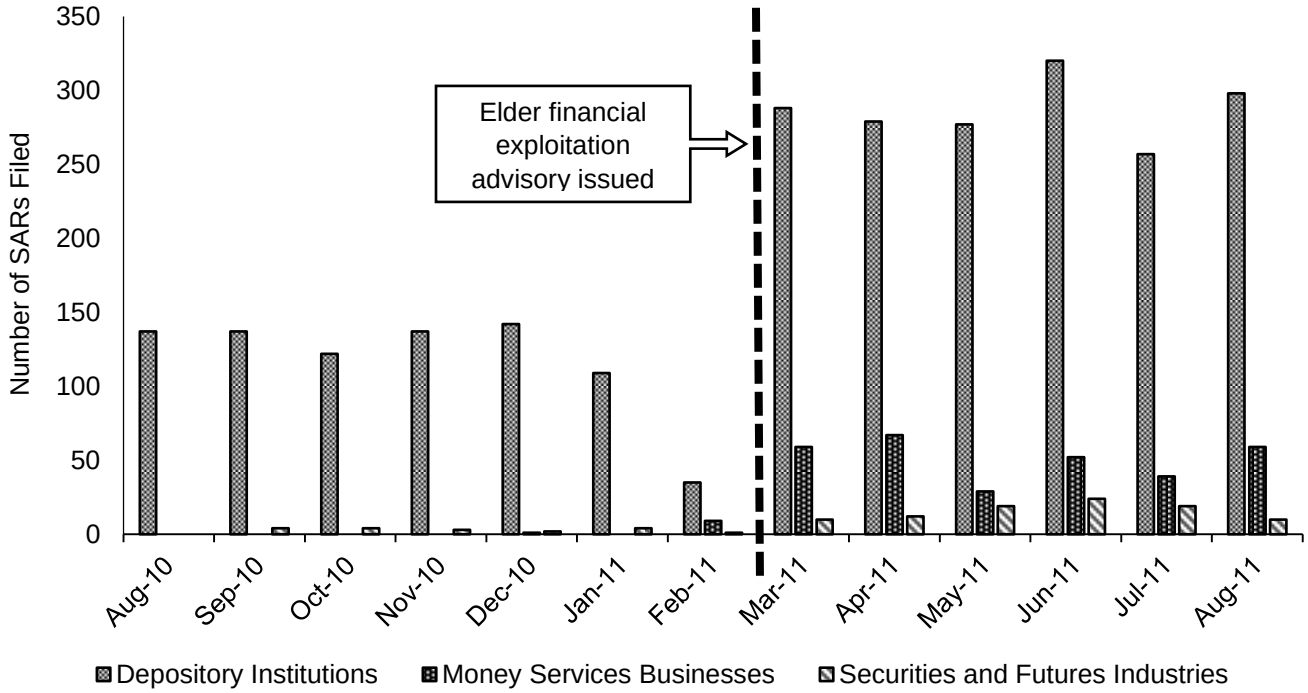

Figure 1. Increase in SAR filings containing the phrase 'elder financial exploitation' following FinCEN Advisory FIN-2011-A003 (August 2010 – August 2011)

Source: FinCEN (2013). SAR Activity Review: Trends, Tips & Issues. *BSA Advisory Group.* Issue 23. Available at https://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf

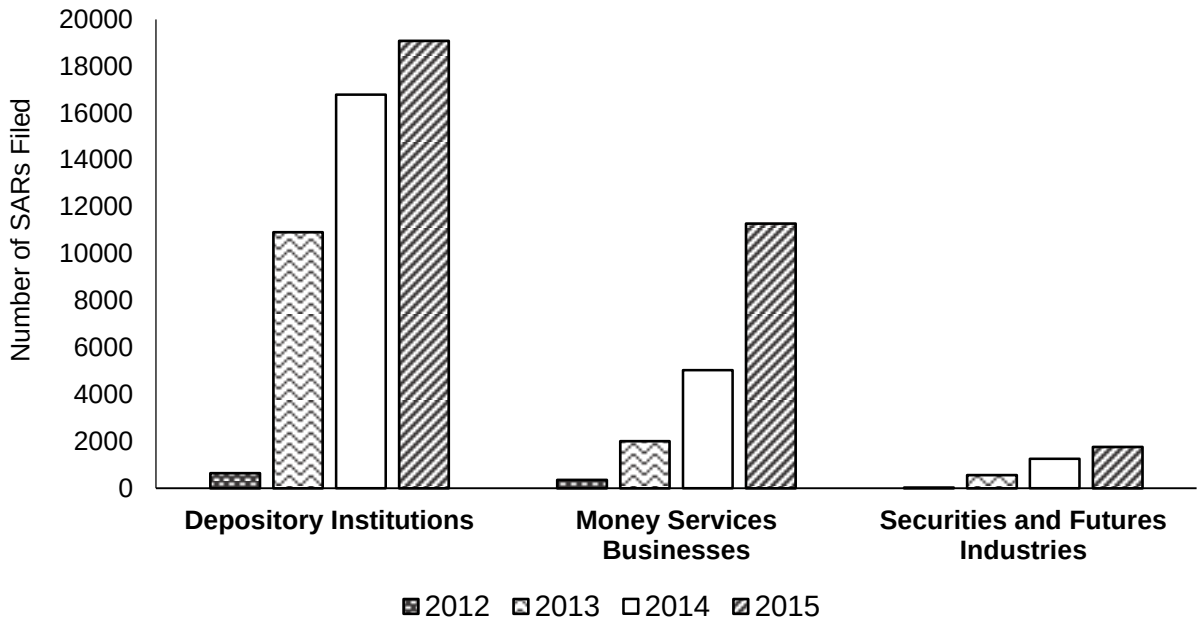

Figure 2. Increase in SARs filings containing the phrase 'elder financial exploitation' from 2012 to 2015 by type of financial service institution.

Source: Author calculations using FinCEN (2016) data publically available at https://www.fincen.gov/Reports/SARStats

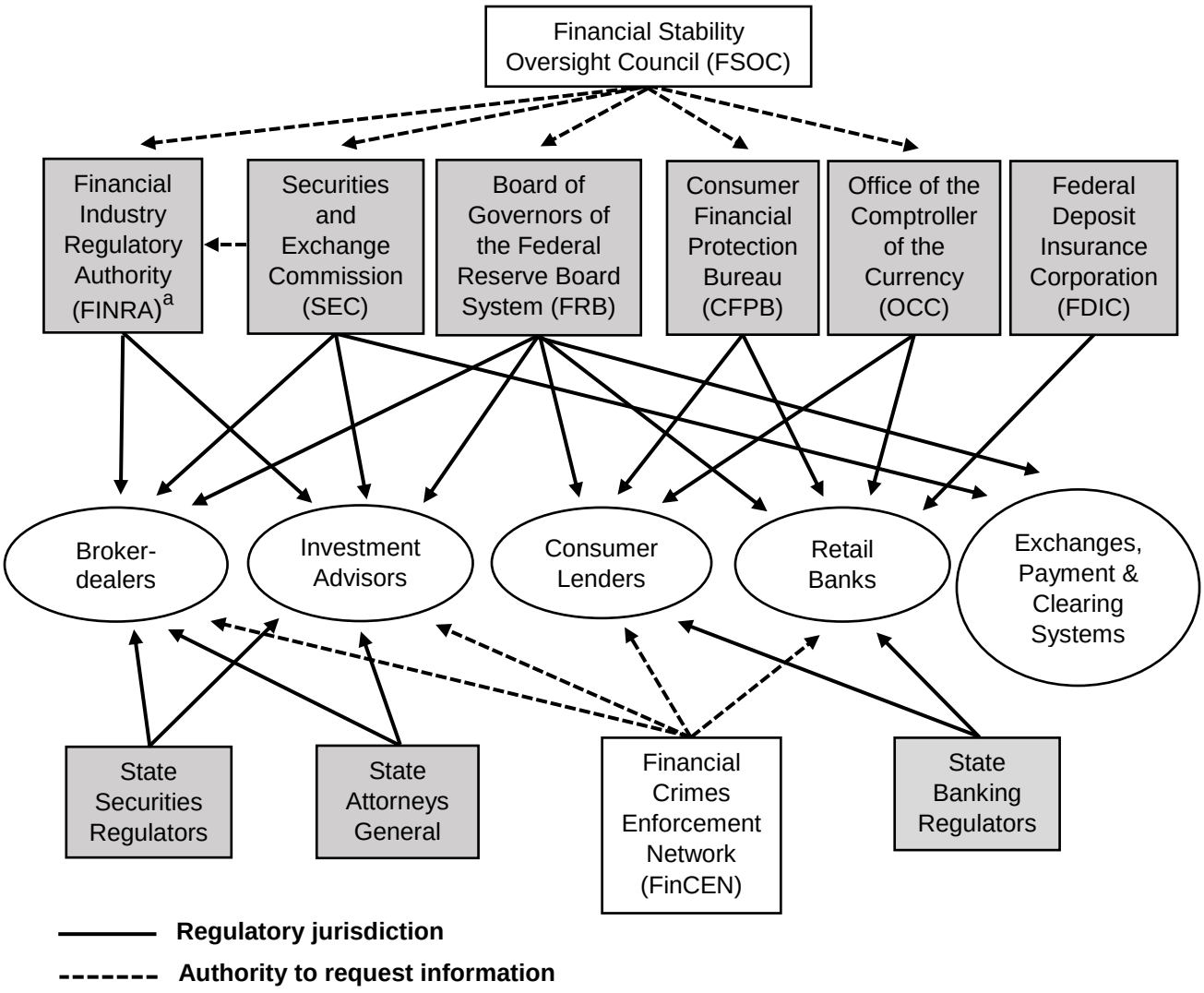

Figure 3. Regulatory oversight of select financial service providers.

Note: Although not depicted in the figure, other agencies have jurisdiction over the financial service industry such as the Commodity Futures Trading Commission, among others**.** There are also other types of financial service providers—e.g., investment banks, commercial lenders, insurance companies—that are not depicted here. Figure 3 excludes providers that do not offer direct services to consumers and their associated oversight agencies because these organizations are outside the scope of the paper.

[a] FINRA is a self-regulatory organization (SRO), a non-governmental, membership-based organization that has the power to create and enforce security regulations and standards. While the SEC is responsible for ensuring fairness for individual investors, FINRA is responsible for overseeing U.S. stockbrokers and brokerage firms.

Source: JP Morgan Chase (2014)