March 2016

Recommendations and report for financial institutions on preventing and responding to elder financial exploitation

Table of contents

Executive Summary

Elder financial exploitation has been called the crime of the 21st century and deploying effective interventions has never been more important. Older people are attractive targets because they often have assets and regular income. These consumers may be especially vulnerable due to isolation, cognitive decline, physical disability, health problems, or bereavement. Elder financial exploitation robs victims of their resources, dignity and quality of life—and they may never recover from it.

Financial institutions play a vital role in preventing and responding to this type of elder abuse. Banks and credit unions are uniquely positioned to detect that an elder account holder has been targeted or victimized, and to take action.

The Consumer Financial Protection Bureau's (CFPB or Bureau) Office for Older Americans has identified best practices to assist financial institutions with their efforts to prevent elder financial abuse and intervene effectively when it occurs. To help financial institutions, the CFPB provides recommendations for banks and credit unions to accompany the Advisory for Financial Institutions on Preventing and Responding to Elder Financial Exploitation, issued simultaneously.[1] The CFPB recognizes that financial institutions vary in size and that the

[1] The Advisory and the Recommendations and report are not intended to interpret federal consumer financial law or any other statute or rule. They are not designed to implement or prescribe any law or Bureau policy. They are not binding on the Bureau or on financial institutions.

protocol, policies and procedures that an institution adopts will likely vary based upon the institution's size and risks.

Key recommendations include:

- **Train management and staff to prevent, detect and respond.** Train personnel regularly and frequently, and tailor training to specific staff roles. Training should cover warning signs that may signal financial exploitation, including behavior and transactions that are red flags, and action steps to prevent exploitation and respond to suspicious events.

- **Use technology to monitor for signs of elder financial exploitation.** Because indicators of elder fraud risk may differ from conventionally accepted patterns of suspicious activity, financial institutions using predictive analytics should review their filtering criteria against individual account holders' patterns and explore additional risk factors that may be associated with elder financial exploitation.

- **Report all cases of suspected exploitation to relevant federal, state and local authorities.** Make timely reports whenever financial institutions spot activity that signals financial exploitation, regardless of whether reporting is mandatory or voluntary under state or federal law. Reporting does not, in general, violate the privacy provisions of the Gramm-Leach-Bliley Act.

- **File Suspicious Activity Reports (SARs).** The Financial Crimes Enforcement Network (FinCEN) issued an Advisory in 2011 noting that SARs are a valuable reporting avenue for these cases. FinCEN now designates "elder financial exploitation" as a category of suspicious activity and provides a checkbox for it on the electronic SAR form. File SARs for elder financial exploitation when mandatory under the Bank Secrecy Act and consider filing them voluntarily in other cases.

- **Expedite documentation request**s from Adult Protective Services (APS), law enforcement and other government entities investigating reports of financial exploitation. Provide documents at no charge.

- **Comply with the Electronic Fund Transfer Act (EFTA) and Regulation E.** Per Regulation E, extend time limits for consumer notification of an unauthorized transaction under extenuating circumstances such as hospitalization. Do not impose

greater consumer liability than Regulation E allows, even when an older consumer may appear to be negligent by, e.g., noting a PIN on or near a debit card.

- **Enable older account holders to consent to information sharing with trusted third parties.** Establish procedures so consumers can provide advance consent to sharing account information with a designated trusted third party when the financial institution reasonably believes that the consumer may be at risk of financial abuse.

- **Offer age-friendly services that can enhance protections against financial exploitation**. Provide consumers with information about planning for incapacity. Honor powers of attorney unless there is a basis in state law to refuse them. Offer opt-in account features such as cash withdrawal limits, geographic transaction limits, alerts for specified account activity, and view-only access for authorized third parties. Where appropriate, offer multi-party accounts without right of survivorship (convenience accounts or agency accounts) as good alternatives to traditional joint bank accounts.

- **Work with law enforcement and Adult Protective Services.** Develop relationships with law enforcement and APS personnel to facilitate timely response to reports. Provide expert consultation and document review to assist with case investigations, including through multidisciplinary teams engaging in case review.

- **Coordinate efforts to educate older account holders, caregivers and the public.** Work with an array of agencies and service organizations to offer educational programs and distribute materials. Participate in multidisciplinary network initiatives.

Financial institutions have a tremendous opportunity to serve older consumers by vigorously protecting them from financial exploitation. The CFPB looks forward to continuing to work with financial institutions and seeing a broad spectrum of financial institutions implement its recommendations so that a greater number of older Americans can enjoy later life economic security.

1. Introduction

1.1 Financial institutions are key actors in combatting elder financial exploitation

Elder financial exploitation has been called "the crime of the 21st century."[2] Deploying effective interventions has never been more important.[3]

Financial institutions play a vital role in preventing and responding to elder financial abuse. Banks and credit unions are uniquely positioned to do so because:

- They know their customers and members
- They often have the opportunity for face-to-face interaction with older consumers who make transactions[4]

---

[2] MetLife Mature Markets Institute, *The MetLife Study of Elder Financial Abuse Crimes of Occasion, Desperation, and Predation Against America's Elders* (June 2011), *available at* https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf.

[3] The population age 65 and over is expected to reach nearly 75 million, or one fifth of the total population, by 2030. CFPB analysis of Census Bureau, National Population Projections, Table 3. Projections of the Population by Sex and Selected Age Groups for the United States: 2015 to 2060 (2014), *at* http://www.census.gov/population/projections/data/national/2014/summarytables.html.

- They are uniquely positioned to detect that an elder account holder has been targeted or victimized
- They are mandated reporters of suspected elder financial exploitation under many states' laws,
- FinCEN states that Suspicious Activity Reports (SARs) are useful for spotting elder financial exploitation and are required when the dollar threshold and other Bank Secrecy Act requirements are met.[5]

The CFPB's Office for Older Americans has identified best practices to enable financial institutions to prevent elder financial abuse and intervene effectively when it occurs. Implementing standards of practice for addressing elder financial exploitation will assist financial institutions in protecting older account holders.

While some banks and credit unions have a comprehensive approach to protecting their older account holders, many still have room for improvement. The CFPB commends those financial institutions across the country that are already reporting elder financial exploitation to the appropriate authorities and making other efforts to protect older consumers.

The CFPB provides broad recommendations in this report to help banks and credit unions prevent and respond quickly to elder financial exploitation.[6] This report accompanies the

---

[4] Older consumers, especially those over age 70, are much more likely than other age groups to rely on tellers as their primary form of banking. FDIC, *2013 FDIC National Survey of Unbanked and Underbanked Households* (Oct. 2014), *available at* https://www.fdic.gov/householdsurvey/2013report.pdf.

[5] FinCEN is a Bureau of the U.S. Department of the Treasury. FinCEN, FIN-2011-A003, *Advisory to Financial Institutions on Filing Suspicious Activity Reports on Elder Financial Exploitation* (Feb. 22, 2011), *available at* https://www.fincen.gov/statutes_regs/guidance/pdf/fin-2011-a003.pdf (hereinafter referred to as FIN-2011-A003, *Advisory to Financial Institutions*) (interpreting 31 CFR §1020.320).

[6] Although this report emphasizes the importance of compliance with appropriate federal and state laws, it is not intended to provide legal advice or serve as a substitute for financial institutions' own legal counsel.

Bureau's Advisory for financial institutions on preventing and responding to elder financial exploitation, issued simultaneously. The CFPB invites institutions to consider the practices identified here as they assess their own current practices.

1.2 Methodology

To prepare its Advisory and this report, the CFPB conducted in-depth, unstructured interviews with a broad spectrum of stakeholders, including representatives of individual banks and credit unions of various sizes, trade associations, technology vendors, law enforcement, prosecutors, adult protective services, aging groups, other federal agencies, and state government entities, over the period of May 2014 to March 2016.

In addition to the interviews, the CFPB reviewed numerous elder financial exploitation training curricula (from individual financial institutions, state bankers associations, national trade associations, state agencies, inter-disciplinary networks, and non-profit organizations) and protocols.

The Bureau developed this set of recommendations by combining the knowledge gained through these activities with its expertise regarding elder financial exploitation.

2. Background

2.1 What is elder financial exploitation?

Elder financial exploitation is the illegal or improper use of an older person's funds, property or assets.[7] Studies suggest that financial exploitation is the most common form of elder abuse and yet only a small fraction of incidents are reported.[8] Estimates of annual losses range from $2.9 billion[9] to $36.48 billion.[10] Perpetrators who target older consumers include, among others,

---

[7] HHS, Nat'l Ctr. on Elder Abuse, Admin. On Aging, *Types of Abuse,Financial or Material Exploitation*, http://www.ncea.aoa.gov/FAQ/Type_Abuse/index.aspx (last visited Feb. 2, 2016).

[8] Ron Acierno, et al., Prevalence and Correlates of Emotional, Physical, Sexual and Financial Abuse and Potential Neglect in the United States: The National Elder Mistreatment Study, 100 Am. J. Pub. Health 292–97 (Feb. 2010), available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2804623/; Lifespan of Greater Rochester, Inc., et al., Under the Radar: New York State Elder Abuse Prevention Study (May 2011), available at http://ocfs.ny.gov/main/reports/Under%20the%20Radar%2005%2012%2011%20final%20report.pdf.

[9] MetLife Mature Market Institute, The MetLife Study of Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation Against America's Elders (June 2011), available at https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf.

[10] True Link Financial, *The True Link Report on Elder Financial Abuse 2015* (Jan. 2015), *available at https://truelink-wordpress-assets.s3.amazonaws.com/wp-content/uploads/True-Link-Report-On-Elder-Financial-Abuse-012815.pdf*. For a discussion of the MetLife and True Link methodologies, *see* Tobie Stanger, *Financial Elder Abuse Costs $3 Billion a Year. Or is it 36 billion?*, Consumer Reports, Sept. 29, 2015,

family members, caregivers, scam artists, financial advisers, home repair contractors, and fiduciaries (such as agents under power of attorney and guardians of property).[11]

Older people are attractive targets because they may have accumulated assets or equity in their homes and usually have a regular source of income such as Social Security or a pension. In 2011, the net worth of households headed by a consumer age 65 and older was approximately $17.2 trillion, and the median net worth was $170,500.[12] These consumers may be especially vulnerable due to isolation, cognitive decline, physical disability, health problems, and/or the recent loss of a partner, family member, or friend.

Cognitive impairment is a key factor in why older adults are targeted and why perpetrators succeed in victimizing them. Even mild cognitive impairment (MCI) can significantly impact the capacity of older people to manage their finances and to judge whether something is a scam or a fraud. Mild cognitive impairment is an intermediate stage between the expected cognitive decline of normal aging and the more serious decline of dementia.[13] Studies indicate that 22 percent of Americans over age 70 have MCI and about one third of Americans age 85 and over have Alzheimer's disease.[14]

---

http://www.consumerreports.org/cro/consumer-protection/financial-elder-abuse-costs--3-billion-----or-is-it--30-billion-.

[11] Tobie Stanger, *Lies, Secrets and Scams: How to Prevent Elder Abuse*, Consumer Reports, Oct. 5, 2015, http://www.consumerreports.org/cro/consumer-protection/preventing-elder-abuse.

[12] *See* US Census Bureau, Table 5, *Mean Value of Assets for Households by Type of Asset Owned and Selected Characteristics: 2011* (2011), http://www.census.gov/people/wealth/files/Wealth_Tables_2011.xlsx (last visited March 15, 2016).

[13] Mayo Clinic, *Mild cognitive impairment* (MCI), http://www.mayoclinic.org/diseases-conditions/mild-cognitive-impairment/basics/definition/con-20026392 (last visited Feb. 8, 2016).

[14] Brenda L. Plassman, et al., *Prevalence of Cognitive Impairment without Dementia in the United States*, 148 Annals Intern. Med. 427-34 (Mar. 2008), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2670458/;

Elder financial exploitation robs victims of their resources, dignity and quality of life. After being exploited, their physical and emotional health may be impacted; they may lose their independence and even have a shortened lifespan; and, they often are unable to replace stolen money or assets because of limited income and no way to rebuild their savings or home equity. Financial exploitation imposes societal costs as well since older victims are more likely to turn to government programs for health and long-term care services.[15]

Since elder financial exploitation takes many different forms, it can be hard to identify. An array of "red flags," however, may signal exploitation. Some of these warning signs are behavioral or interpersonal—for example, an older person appears to be submissive or fearful of a caregiver. Some signals are transactional, such as frequent large withdrawals from an account or uncharacteristic requests to wire money.[16]

Alzheimer's Ass'n, *2015 Alzheimer's Disease Facts and Figures, available at* https://www.alz.org/facts/downloads/facts_figures_2015.pdf.

[15] Janey C. Peterson, et al., *Financial Exploitation of Older Adults: A Population-Based Prevalence Study*, 29 J. Gen. Intern. Med. 1615, 1620-21 (2014), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4242880/pdf/11606_2014_Article_2946.pdf; Jilenne Gunther, *The 2011 Utah Economic Cost of Financial Exploitation*(2011), *available at* http://victimsofcrime.org/docs/default-source/financial-fraud/2011-economic-cost-of-financial-exploitation.pdf?sfvrsn=2; Bryan J. Kemp & Laura A. Mosqueda, *Elder Financial Abuse: An Evaluation Framework and Supporting Evidence*, 53 J. Am. Geriatr. Soc. 1123, 1123 (July 2005), *available at* http://www.centeronelderabuse.org/docs/EldFinAbuse_KempMosqueda2005.pdf; Brian K. Payne, *Crime and Elder Abuse: An Integrated Perspective* (3 ed. 2011); Charles C. Thomas, World Health Organization, *European Report on Preventing Elder Maltreatment* (2011), *available at* http://www.euro.who.int/_data/assets/pdf_file/0010/144676/e95110.pdf; Ronan M. Factora, *Aging and Money: Reducing Risk of Financial Exploitation and Protecting Financial Resources* (2014).

[16] *See also*, FinCEN, *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions*, Version 1.2 (Oct. 2012), *available at* https://www.fincen.gov/forms/files/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf (hereafter referred to as FinCEN *Suspicious Activity Report*); Fed. Reserve, CFTC, CFPB, FDIC, FTC, NCUA, OCC, *Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults* (Sept. 23, 2013), *available at* http://files.consumerfinance.gov/f/201309_cfpb_elder-abuse-guidance.pdf (hereinafter *Interagency Guidance on Privacy Laws*).

2.2 Case Scenarios

The following are a few case examples from news reports to illustrate the ways that a variety of perpetrators exploit older consumers. In all of these cases, funds went from the victims' deposit accounts to the perpetrators.

- A Minnesota pastor persuaded a man suffering from Alzheimer's and Parkinson's diseases to allow him to manage his finances. The pastor made over 130 withdrawals from the older man's bank account and was later convicted of stealing about $25,000.[17]

- Prosecutors charged an Indiana home care worker with nine felonies after she took more than $150,000 from a 79-year-old woman with dementia. The caregiver stole the funds through transactions on multiple credit cards, checks drawn on a savings account and cashed certificates of deposit. A bank fraud analyst was the first to detect the unusually large credit card charges, and the analyst called Indiana Adult Protective Services.[18]

- An Oklahoma woman received mail and phone calls telling her that she had won a sweepstakes and would get prizes if she sent money to collect her winnings. She sent as many as 90 checks a month, in response to requests for payments of $50 to $2,000. A bank employee discovered the losses when the victim asked how she could send a large amount of cash through the mail.[19]

---

[17] *St. Paul pastor sentenced for stealing from parishioner*, StarTribune, Sept. 14, 2012, *available at* http://www.startribune.com/local/east/169851546.html.

[18] Marisa Kwiatkowski, *Financial exploitation cases burden seniors, Indiana*, Indianapolis Star, Jan. 17, 2016, *available a* http://www.indystar.com/story/news/investigations/2016/01/17/financial-exploitation-cases-burden-seniors-indiana/78810678/.

[19] US Postal Inspection Serv., *US Postal Inspectors warn seniors against sweepstakes scams: You're a Guaranteed Loser!*, https://postalinspectors.uspis.gov/radDocs/victim.htm (last visited Feb. 8, 2016).

3. Recommendations

3.1 Develop, implement, and maintain internal protocols and procedures for protecting account holders from elder financial exploitation

The CFPB recommends that financial institutions develop a protocol for management and staff to follow to prevent and respond to suspected cases of elder financial exploitation.

The protocol should include key policies and procedures regarding the following topics:

- Training requirements and resources
- Reporting to appropriate federal, state and local entities, including
  - Process for frontline or other staff to flag suspicion to relevant management and other personnel
  - Responsibilities of management and staff for communication with the account holder and investigating suspicious activity
  - Designation of responsibilities for reporting to Adult Protective Services (APS), law enforcement and other entities
  - Information on what to include in reports, and
  - Responding to records requests from external entities performing investigations
- Regulation E compliance

- Procedures for sharing account information with third parties
- Ongoing collaboration with external stakeholders.

The CFPB recognizes that financial institutions vary in size and that the protocol, policies and procedures that an institution adopts will likely vary based upon the institution's size and risks.

3.2 Train employees

Training employees is critical in the effort to prevent, detect and respond to elder financial exploitation. Clear, efficient training protocols enhance financial institutions' capacity to detect elder financial exploitation. It is essential that training programs describe what actions to take when employees detect problems. Training should communicate the roles and responsibilities of management, frontline staff, and other employees to reduce ambiguity and promote efficient and timely action when staff suspect or observe elder financial exploitation.[20]

The CFPB recommends the following practices for all employee training programs:

3.2.1 Elder financial exploitation training curriculum components

Training curricula should build on existing fraud training programs and articulate characteristics of elder financial exploitation that make it unique and difficult to detect. The following elements comprise a minimum foundation in elder financial exploitation training:

---

[20] *See*, e.g., The Maine Reporting Project for Financial Institutions, *Fighting Financial Exploitation, Trainer Reference Manual* 1-4, 3rd ed. (2014), *available at* http://www.maine.gov/dhhs/oads/trainings-resources/publications.html (follow link to Microsoft Word version of The Maine Reporting Project for Financial Institutions).

Definition of elder financial exploitation

The CFPB recommends that financial institutions adopt a comprehensive definition of elder financial exploitation. A multifaceted definition provides trainees with a sense of the varied and nuanced forms that exploitation can take.[21] For example, misappropriation of an older person's account funds and coercing a senior to co-sign on a loan are both forms of elder financial exploitation.[22]

The CFPB recommends that financial institutions incorporate relevant state-specific definitions into their training since definitions often vary by state. It is critical, for example, for staff to know the definition of elder financial exploitation in their state's APS laws.[23] If the state criminal code defines elder financial exploitation as a crime, knowing that definition can help staff as they prepare reports to law enforcement.

Indicators of potential elder financial exploitation

Signs of elder financial exploitation may differ from the indicators of other fraud types. Accordingly, it is important for training curricula to include categorical descriptions of how exploitation can occur and the red flags to watch for in each category.[24] This report includes a

---

[21] For example, as defined in the Older Americans Act, exploitation is "the fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual, including a caregiver or fiduciary, that uses the resources of an elder for monetary or personal benefit, profit, or gain, or that results in depriving an elder of rightful access to, or use of, benefits, resources, belongings, or assets." 42 U.S.C. § 1397j(8).

[22] Oregon Bankers Ass'n & Oregon Dep't Hum. Serv., *Preventing Elder Financial Exploitation: How Banks Can Help*, (4th ed. June 2013), *available at* http://www.oregonbankers.com/uploads/5/1/5/1/51510679/2013_elder_abuse_manual_-_web_version_-_final.pdf.

[23] *See infra* Report suspected activity, Adult Protective Services at 3.4.5.

[24] *See* App. A for additional red flags of elder financial exploitation. *See also* BITS Financial Services Roundtable, *Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation* (Apr. 2010) 11-14, *available at*

list of warning signs that may indicate elder financial exploitation, at Appendix A. Examples of red flag categories include, but are not limited to:

- Transaction pattern changes:
  - Abrupt increases in withdrawals; new spending patterns following the addition of a new authorized user; atypical ATM withdrawals; unusual gaps in check numbers.
- Identity theft and coercion:
  - Address changes followed by account changes; new third party speaking for the older adult; older consumer is confused by or unaware of account changes; requests to send account statements to a third party's address.
- Behavioral changes:
  - Older consumer appears newly distressed, unkempt, or unhygienic; older consumer mentions lottery or sweepstakes opportunities or winnings; older adult inquires about international wire transfers.

Using vignettes or case studies to illustrate plausible scenarios may enable staff to understand and remember the red flags.[25]

---

http://fsroundtable.org/wp-content/uploads/2015/05/BITSProtectingVulnerableAdults0410.pdf; Coalition for Elder Justice in Connecticut, *Preventing Elder Financial Exploitation* (Feb. 2015) 26-34, http://coa.cga.ct.gov/images/pdf/financialabuse/ElderJusiticeFinancialInstitutionsTraining2.12.15.pdf; Mark S. Lachs & Karl A. Pillemer, *Elder Abuse*, 373 N. Engl. J. Med. 1947 (2015), *available at* http://www.nejm.org/doi/full/10.1056/NEJMra1404688.

[25] CFBP and FDIC, *MoneySmart for Older Adults: Participant Resource Guide* (Jun. 2013), http://files.consumerfinance.gov/f/201306_cfpb_msoa-participant-guide.pdf.

Action steps for preventing elder financial exploitation

It is critical for financial institutions to train employees on how to take preventive measures against elder financial exploitation in addition to responsive or reactive processes. Training can articulate a spectrum of proactive steps to take depending on the situation encountered by the employee. Examples of preventive measures include, but are not limited to:

- Asking customers to explain and confirm transactions that raise red flags, e.g.:
  - With a large cash withdrawal ("This is an unusually large withdrawal, are you sure you want cash?")
  - With wire transfers, ("Have you taken steps to be sure the recipient is trustworthy?")
  - With large online transactions ("I'm calling to confirm your recent online banking activity because the transfer is a large amount.")
  - When a third party accompanies the account holder and other red flags are present ("Can we talk privately for a moment?")
- Instructions for recognizing signs of diminished capacity with action steps for frontline staff to follow when signs are observed in customers[26]
  - Examples such as memory loss, communication problems, calculation problems and disorientation may be signs of diminished capacity in a customer

[26] SEC, Office of Compliance Inspections and Examinations, North American Securities Administrators Ass'n & Financial Industry Regulatory Authority, *Protecting Senior Investors: Compliance, Supervisory and Other Practices Used By Financial Services Firms in Serving Senior Investors* 7-8 (2008), *available at* http://www.nasaa.org/wp-content/uploads/2010/08/SEC-NASAA_Senior_Report_092208.pdf; American Bar Association, Recognizing and dealing with diminished capacity in older clients, http://www.americanbar.org/news/abanews/aba-news-archives/2013/10/recognizing_and_deal.html (last visited Feb. 17, 2016).

- Educating older customers on common scams and fraud ("Have you read up on the latest telemarketing scams? Here's a flyer to take home and to share with friends and family.")

Action steps for responding to suspected elder financial exploitation

The CFPB recommends that financial institutions train staff to respond quickly when they suspect elder fraud and to follow clear, detailed action steps.[27] To enhance timely response and enable quick reporting, the CFPB recommends that training include:

- Tips on immediate steps for frontline staff, such as scripted questions to ask customers, calling 911 if the account holder appears to be in immediate danger, and instructions for effectively documenting details
- Internal response sequences for alerting appropriate staff throughout the organizational hierarchy, e.g.:
  - Alerting peer staff, supervisory staff, management, security and compliance staff, as appropriate and according to the financial institution's protocol
- Action steps for reporting to law enforcement, APS, and other external entities (*see infra* at 3.4). Financial institutions may wish to provide staff with quick reference guides with rules and tips for reporting to law enforcement and APS. Including state-specific information on APS and other agencies' jurisdiction and procedures could enhance understanding and efficiency.[28]

---

[27] MO Dept. of Health & Senior Services, *MO$AFE: Missourians Stopping Adult Financial Exploitation* 12-22 (Aug. 2005), *available at* http://health.mo.gov/seniors/mosafe/pdf/MOSAFEResourceManual.pdf; CA Dept. of Justice, *A Citizen's Guide to Preventing and Reporting Elder Abuse 20-34* (2002), *available at* http://ag.ca.gov/bmfea/pdfs/citizens_guide.pdf.

[28] *See infra* Report suspicious activity at 3.4.

- Steps for filing detailed Suspicious Activity Reports (SARs) with detailed and relevant supporting documentation, and for maintaining relevant documentation in accordance with BSA requirements (*see infra* at 3.4.3).[29]
- Steps for alerting trusted third parties (*see infra* at 3.5.2).
- Tips for being an effective witness of suspicious behavior, e.g., keeping detailed contemporaneous notes on observations.

3.2.2 Tailor trainings for different staff roles

Financial institution employees have varying expertise, authority, and public-facing duties based on their positions within the organizational structure. Employees in some institutions may perform multiple roles or have overlapping job duties. For these institutions, a generalized approach to training may be the most efficient system. When applicable, large institutions—and other institutions that assign specific responsibility for investigation, reporting and other duties—should tailor training programs to fit staff roles and responsibilities. Customized training prepares employees to react to events they are most likely to encounter and act on in their respective positions. For example, frontline staff directly observe and engage customers. Training for these employees could emphasize red flag detection and the alerting of key personnel. Tailored training for supervisory employees could, by contrast, focus on external reporting protocols and requirements.

[29] FinCEN *Suspicious Activity Report*, *supra*; FinCEN Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative 13-21, https://www.fincen.gov/news_room/rp/files/sar_guidance_narrative.pdf (hereafter referred to as FinCEN Guidance on Preparing SARs); FIN-2011-A003, *Advisory to Financial Institutions*, *supra*.

3.2.3 Repeat training periodically

Studies show that repetitive training deepens the learning process and improves memory retention.[30] Cyclical, repetitive training can reinforce individual knowledge and increase collective expertise within institutions.[31]

The CFPB recommends that financial institutions incorporate elder financial exploitation training and retraining cycles into their institutional culture. In addition to enhanceing knowledge retention, cyclical retraining may help to integrate elder financial issues into the daily language and awareness of staff. Frequent training cycles may also help new employees learn this subject matter.[32]

3.3 Detect elder financial exploitation by harnessing technology

There are two main avenues for detecting signs that may indicate elder financial exploitation. Tellers and other public-facing staff are essential for spotting signs of financial exploitation, particularly behavioral signs they notice when interacting with older account holders and third

---

[30] Jurgen Kornmeir, Manfred Spitzer& Zrinka Sosic-Vasic, *Very Similar Spacing-Effect Patterns in Very Different Learning/Practice Domains* 1, Plos One, Vol 9, Issue 3 (Mar. 2014), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3946552/pdf/pone.0090656.pdf.

[31] Jeffrey D. Karpicke & Althea Bauernschmidt, *Spaced Retrieval: Absolute spacing enhances learning regardless of relative spacing*, 37 J. Exp. Psychology: Learning, Memory, and Cognition 1250 (2011), *available at* http://learninglab.psych.purdue.edu/downloads/2011_Karpicke_Bauernschmidt_JEPLMC.pdf.

[32] For example, BITS Financial Services Roundtable recommends: initial training for all new employees; thorough annual training; and, quarterly communications to reinforce messages, such as one-page tip documents. BITS Financial Services Roundtable, *At-Risk Adult Training Curriculum* (2013), *available at* http://fsroundtable.org/wp-content/uploads/2015/09/BITS-Roundtable-At-Risk-Adult-Training-Curriculum-Jan-2013.pdf.

parties. (*See supra* at 3.2.1 and *infra* at Appendix A.) The other key approach to detection is utilizing technology to flag transactions or account activity that may signal financial abuse.

Financial institutions can utilize existing suspicious activity monitoring technology to detect elder financial exploitation. The CFPB encourages financial institutions to ensure that their systems include analyses of the types of products and account activity that may be associated with elder financial exploitation risk.

Financial institutions perform transaction monitoring, tracking, reporting, and recordkeeping on customer account data. These actions support Bank Secrecy Act and Anti-Money Laundering (BSA/AML) compliance, and can also help to prevent fraud. The internal controls that financial institutions have implemented in furtherance of the BSA/AML obligations include effective detection capabilities that can recognize distinct risk indicators for elder fraud.

Suspicious activity monitoring programs typically include a combination of both manual and automated systems to detect unusual activity. Manual fraud detection systems operate by programming rules that flag specific events identified in account activity for further review by staff. For example, the program may flag cash withdrawals over a set limit or international transactions as suspicious. These are valuable techniques, but they use static, predetermined rules that may miss specific transactions that are unusual for a particular account holder.

In the last two decades, financial institutions have increasingly adopted sophisticated automated fraud detection systems using machine learning technology. Machine learning analyzes transactions in relation to historical account activity and programmed parameters.[33] The programs are said to "learn" statistical patterns in account data and can recognize real-time

---

[33] Fed. Fin. Inst. Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* 61-67(2014), https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf; Jesus Mena, *Machine Learning Forensics for Law Enforcement, Security, and Intelligence* 1-24 (CRC Press, 2011); telephone interview with Dale Smith, Data Scientist, Nexidia Inc. (Oct. 14, 2015) and telephone interview with Steven Vallejo, Corporate Security Director, Bank of the West (Oct. 28, 2015).

deviations in these patterns on individual accounts.[34] As the system detects anomalies, it measures their risk potential according to its programmed tolerances or filtering criteria. The filtering criteria determine whether the system flags the activity for review.[35]

Some indicators of elder fraud risk may not match conventionally accepted patterns of suspicious activity, but nevertheless may be unusual in light of a particular account holder's regular pattern of behavior. Financial institutions can ensure that their systems consider the type of account-related activity that may be associated with elder fraud risk. The following is a sample of the types of account activity that may be associated with elder financial exploitation:[36]

- Atypical ATM card use
- Uncharacteristic non-sufficient funds activity or overdraft fees
- Activity in previously inactive accounts
- Change of address on account
- Opening new joint checking account or adding joint owner to existing account
- Increase in total monthly cash withdrawals compared to historical patterns

---

[34] Ethem Alpaydin, Introduction to Machine Learning (3rd edition, 2014); Jesus Mena, Machine Learning Forensics for Law Enforcement, Security, and Intelligence 7 (2011).

[35] In some cases automated systems are able to alert financial institution employees to a transaction before it is completed. Mena, *supra* note 34, at 10-14.

[36] BITS Financial Services Roundtable, *Protecting the Elderly and Vulnerable from Financial Exploitation* 11-13 (2010), *available at* http://fsroundtable.org/wp-content/uploads/2015/05/BITSProtectingVulnerableAdults0410.pdf; E-mail from Howard L. Tischler, C.E.O., and E. Elizabeth Loewy, General Counsel & Sr. V.P. of Industry Relations, Eversafe, to the CFPB (Sept. 21, 2015) (on file with the CFPB).

- Automated Clearing House (ACH) payment to a recipient with no history of ACH transactions with the customer
- Missing recurring deposits
- Electronic bill payments to new vendors
- Atypical use of online banking
- Atypical use of wire transfers
- Unusual gaps in check numbers.

The CFPB encourages financial institutions using predictive analytics to review their filtering criteria against individual account holders' patterns and to explore additional risk factors that may be associated with elder financial exploitation.

3.4 Report suspicious activity

3.4.1 Report all cases of suspected elder financial exploitation

The CFPB recommends that financial institutions report suspected financial exploitation of older adults to all appropriate local, state or federal responders,[37] regardless of whether reporting is mandatory or voluntary under state or federal law.[38]

---

[37] Federal responders might include the US Postal Inspection Service and the Federal Bureau of Investigation.

[38] *See infra* at 3.4.4. regarding privacy law considerations related to reporting financial exploitation.

Typically, the institution should file reports with the appropriate APS agency and law enforcement. In addition, financial institutions should file SARs with FinCEN.[39] When the account holder resides in a nursing facility, assisted living facility or similar adult care facility, the financial institution could also consider reporting suspected financial exploitation to the regional or local long-term care ombudsman. See descriptions of these agencies and entities below.

Some financial institutions—including some of the nation's largest banks—have blanket policies treating all cases of suspected financial abuse (regardless of jurisdiction) as if subject to state mandatory reporting laws (*see infra* at 3.4.2). In addition, these policies can enhance consistency in reporting, expedite action and eliminate the extra step of determining whether reporting is mandatory in a given location and situation.

3.4.2 Understand reporting requirements

While the CFPB recommends that everyone in every state report suspected financial exploitation to Adult Protective Services, as of February 2016 only about half the states mandate that financial institutions or a subset of financial professionals report suspected elder financial exploitation to APS, law enforcement or both.[40] Those states include states in which "any person" must report elder financial exploitation.[41] In the remaining states with mandatory

---

[39] FIN-2011-A003, Advisory to Financial Institutions, supra; See *infra* at 3.4.3.

[40] Arizona, Arkansas, California, Colorado, Delaware, District of Columbia, Florida, Georgia, Hawaii, Illinois, Indiana, Kansas, Kentucky, Louisiana, Maryland, Mississippi, Nevada, New Hampshire, New Mexico, North Carolina, Oklahoma, Rhode Island, South Carolina, Tennessee, Texas, Utah, Washington and Wyoming. *See infra* footnotes 41 and 42 for statutory citations. Although this report emphasizes the importance of compliance with appropriate state laws, it is not intended to provide legal advice or serve as a substitute for financial institutions' own legal counsel.

[41] Ind. Code Ann. § 12-10-3-9(a); Ky. Rev. Stat. Ann. § 209.030(2); La. Rev. Stat. Ann. § 1504(A); N.H. Rev. Stat. Ann. § 161-F:46; N.C. Gen Stat. § 108A-102(a); Okla. Stat. Ann. Tit. 43A §10-104(A); R.I. Gen. Laws Ann. § 42-66-8; S.C. Code Ann. § 43-35-25(A); Tenn. Code Ann. § 71-6-103(b)(1); Tex. Hum. Res. Code Ann. § 48.051(b); Utah Code Ann. § 62A-3-305(1); Wyo. Stat. Ann. § 35-20-103(a).

reporting by financial institutions,[42] a statute specifically names financial institutions or certain members of their staff as mandatory reporters. For example, in California a mandated reporter of financial abuse of an elder or dependent adult "includes all officers and employees of financial institutions" and the statute defines financial institutions to include depository institutions and credit unions.[43] A few state statutes are narrower. For example, a "bank manager" and a "financial manager" are mandated reporters in the District of Columbia.[44]

The CFPB recommends that financial institutions determine whether and when state law mandates reporting by the institution. In addition, states may require that oral and/or written reports to APS are made within a certain time period.[45]

Some states mandate that financial institution personnel report suspected elder financial exploitation to law enforcement in addition to APS.[46] Financial institutions should determine whether they have reporting obligations to law enforcement or other agencies (other than APS) under relevant state laws.

---

[42] Ark. Code Ann. § 12-12-1708(a)(1); Cal. Welf. & Inst. Code § 15630.1; Colo. Rev. Stat. § 18-6.5-108(1); Del. Code Ann. Tit.31 § 3910(c); D.C. Code §7-1903(a)(1); Fla. Stat. § 415.1034(1)(a); Ga. Code Ann. § 30-5-4(a)(1)(B); Haw. Rev. Stat. § 412L3-114.5; Kan. Stat. Ann. §39-1431(a); Md. Code Ann. Fin. Inst. § 1-306(d)(1); Miss. Code Ann.§ 43-47-7(1)(a); Nev. Rev. Stat. § 657.290; N.M. Stat. Ann. § 27-7-30(A). In Washington, financial institution employees are only mandated to report financial exploitation when the institution is refusing 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. Rev. Code Wash. § 74.34.215(4). In Illinois, a bank employee is required to report if the employee is a trustee or a licensed public accountant. 320 Ill. Comp. Stat. 20/4. In Arizona reporting is required by "a person who has responsibility for any other action concerning the use or preservation of the vulnerable adult's property" who discovers the exploitation while fulfilling that responsibility. Ariz. Rev. Stat. Ann. § 46-454(B).

[43] Cal. Welf. and Inst. Code § 15630.1.

[44] D.C. Code § 7-1903(a)(1).

[45] *See*, e.g., MD. Code Ann. Fin. Inst. § 1-306.

[46] *See*, e.g., D.C. Code § 7-1903.

Financial exploitation may violate an array of criminal laws. Familiarity with state criminal code provisions will help ensure that financial institutions report suspected criminal acts.

Almost all states have provisions providing immunity for good faith reporting of suspected elder financial exploitation. These "safe harbor" provisions provide immunity even when the activity observed wasn't financial exploitation, as long as the reporter acted in good faith (or a similar standard spelled out in state law). In most states, this immunity extends to civil, criminal, or administrative actions.

Under state laws, a financial institution normally does not need proof that elder financial exploitation is occurring. Reasonable suspicion is adequate.[47] It is the job of Adult Protective Services and/or law enforcement to determine if exploitation is occurring. (*See infra* at 3.4.5.) If the elder appears to be in imminent danger of abuse, staff should call 911 for an immediate police response.

3.4.3 File Suspicious Activity Reports when the financial institution suspects abuse

In February, 2011 FinCEN issued an Advisory to financial institutions on filing suspicious activity reports regarding elder financial exploitation. FinCEN noted that SARs are a valuable avenue for financial institutions to report elder financial exploitation.

> Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Part 103... [now codified at 31 CFR § 1020.320], if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after

---

[47] *See*, e.g., Fla. Stat. § 415.1034(1)(a), which provides "Bank, savings and loan, or credit union officer, trustee, or employee...knows, or has reasonable cause to suspect;" Ga. Code Ann. § 30-5-4(a)(1)(B) provides "any employee of a financial institution...having reasonable cause to believe...."

> examining the available facts, including the background and possible purpose of the transaction, the financial institution should then file a Suspicious Activity Report.[48]

SAR filing is mandatory for banks (defined in FinCEN rules to include credit unions) when certain thresholds are met.[49] If the transaction amounts are below the mandatory filing threshold, consider filing SARs anyway. As FinCEN stated in its 2011 Advisory on Elder Financial Exploitation, "[a] financial institution may also file with FinCEN a Suspicious Activity Report with respect to any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by FinCEN regulations."[50] Voluntary reporting may help deter continued financial abuse by the same perpetrator, and may help law enforcement with ongoing investigations and prosecution.

With the introduction of electronic SAR filing, FinCEN provided a designated category of suspicious activity entitled "elder financial exploitation" for financial institutions to check (option d in field 35 of the form).[51] Prior to the checkbox, FinCEN had requested that financial institutions use the key terms "elder financial exploitation" and "elder financial abuse" in the SAR narrative.[52]

---

[48] FIN-2011-A003, Advisory to Financial Institutions, supra.

[49] 31 CFR § 1020.320(a)(2); 12 CFR §§ 21.11(c)(3), 163.180(d)(3)(iii), 208.62(c)(3), 353.3(a)(3) and 748.1(c)(1)(iii).

[50] FIN-2011-A003, Advisory to Financial Institutions, supra.

[51] FinCEN, FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions, supra at 98.

[52] FIN-2011-A003, *Advisory to Financial Institutions, supra*. Although the FinCEN advisory did not specifically instruct filers to use the latter term, FinCEN wanted to ensure identification of all relevant SARs and thus included the additional phrase in the search.

While financial institutions now note by checkbox that the suspicious activity is elder financial exploitation, the narrative remains extremely important. As FinCEN says in its instructions for filers,

> The narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion.[53]

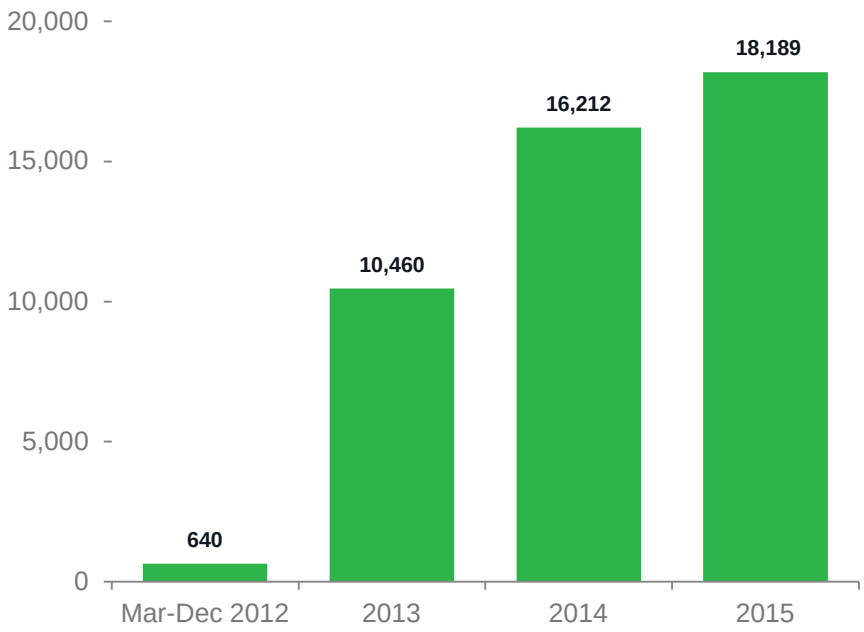
In addition, it is important to note that the potential victim of elder financial exploitation should not be reported as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.[54]

---

[53] FinCEN, *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions*, Version 1.2 (2012) at 110, *available at* https://www.fincen.gov/forms/files/FinCEN%20SAR%20ElectronicFilingInstructions-%20Stand%20Alone%20doc.pdf.

[54] FIN-2011-A003, Advisory to Financial Institutions, supra.

FIGURE 1: TREND IN SARS FILED BY DEPOSITORY INSTITUTIONS ABOUT ELDER FINANCIAL EXPLOITATION [55]



[55] FinCEN, *SAR Stats, Technical Bulletin* (Oct. 2015), *available at* https://www.fincen.gov/news_room/rp/files/SAR02/SAR_Stats_2_FINAL.pdf (follow "SAR Stats - Issue 2 – Depository Institutions" on Table of Contents page for 2012-2014 data; use "Interactive SAR Stats" hyperlink on page 2 for 2015 data)(last visited Feb. 17, 2016). This figure utilizes data collected on the current FinCEN Suspicious Activity Report form (Form 111), which FinCEN made available for filing on March 1, 2012. *SAR Stats* and the *SAR Stats Interactive Module* do not include legacy form data. Therefore the figure does not include data for January and February of 2012. (However, depository institutions do submit SARs continuously throughout the year.)

3.4.4 Understand that the Gramm-Leach-Bliley Act is not a barrier to reporting suspected elder financial exploitation

Financial institutions have expressed concern over whether reporting suspected elder financial exploitation violates the privacy provisions of the Gramm-Leach-Bliley Act (GLBA). Bank officials told the U.S. Government Accountability Office (GAO) in an engagement involving elder financial exploitation that clarification of bank roles and responsibilities related to privacy and financial exploitation of older account holders was needed.[56] Financial institutions repeatedly raised these concerns with CFPB officials in meetings.

To provide financial institutions more certainty about the legality of reporting abuse and to facilitate timely reporting and response, the eight federal regulatory agencies with authority to enforce the privacy provisions of GLBA issued Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults on September 24, 2013 (the Guidance).[57] The Guidance clarifies that reporting financial abuse of older adults to appropriate authorities does not, in general, violate the privacy provisions of GLBA.

GLBA generally requires that a financial institution notify consumers and give them an opportunity to opt out before the institution can disclose nonpublic personal information to a nonaffiliated third party.[58] But there are specific exceptions to the notice and opt-out requirement that may permit information sharing with local, state, or federal agencies to report

---

[56] GAO, Report to Congressional Requesters, *Elder Justice, National Strategy Needed to Effectively Combat Elder Financial Exploitation* (Nov. 2012), *available at* http://www.gao.gov/assets/660/650074.pdf (hereafter GAO, *Elder Justice, National Strategy Needed*).

[57] Fed. Reserve, CFTC, CFPB, FDIC, FTC, NCUA, OCC & SEC, *Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults* (Sept. 23, 2013), *available at* http://files.consumerfinance.gov/f/201309_cfpb_elder-abuse-guidance.pdf (hereafter referred to as *Interagency Guidance on Privacy Laws*).

[58] 15 U.S.C. §§ 6802(a)-(b), 6803(a) and 6803(c); 12 CFR §§ 1016.4 and 1016.10.

suspected elder financial exploitation. At least one of these exceptions likely applies in every case of suspected elder financial exploitation. As stated in the Interagency Guidance,[59] those broad exceptions are:

- To comply with federal, state, or local laws, rules and applicable legal requirements (and these laws include state mandatory reporting laws)[60]
- To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by federal, state, or local authorities[61] or to respond to judicial process or government regulatory authorities having jurisdiction for examination, compliance or other purposes[62]
- To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability[63] (For example, this exception generally would allow a financial institution to disclose to appropriate authorities nonpublic personal information in order to report incidents that result in taking an older adult's funds without actual consent, or report incidents of obtaining an older adult's consent to sign over assets through misrepresentation of the intent of the transaction)
- To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, disclosure to law

---

[59] See Interagency Guidance on Privacy Laws, supra.

[60] 15 U.S.C. § 6802(e)(3)(B); 12 CFR §1016.15(a)(7)(i).

[61] 15 U.S.C. § 6802(e)(8); 12 CFR §1016.15(a)(7)(ii).

[62] 15 U.S.C. § 6802(e)(8); 12 CFR § 1016.15(a)(7)(iii).

[63] 15 U.S.C. § 6802(e)(3)(B); 12 CFR § 1016.15(a)(2)(ii).

enforcement agencies, self-regulatory agencies, or for an investigation on a matter related to public safety.[64]

In addition to these exceptions, financial institutions may disclose nonpublic personal information with the consumer's consent or to the consumer's legal representative or fiduciary.[65]

Financial institutions also should be aware of any state regulatory guidance on privacy laws and reporting financial exploitation. State banking or financial services regulators in several states have issued similar guidance. For example, on April 22, 2014, the Minnesota Department of Commerce issued guidance for Minnesota banks on privacy laws and reporting financial abuse of older adults.[66] The New York State Department of Financial Services issued guidance on February 26, 2015, stating that, in addition to the GLBA exceptions, "New York State law allows financial institutions in New York to report suspected elder financial exploitation to APS or law enforcement."[67]

---

[64] 15 U.S.C. § 6802(e)(5); 12 CFR § 1016.15(a)(4).

[65] 12 CFR § 1016.15(a)(1), 1016.15(a)(2)(v).

[66] MN Dept. of Comm., Guidance on Privacy Laws and the Reporting of Financial Abuse of Older Adults, https://mn.gov/commerce/industries/financial-institutions/privacy-laws-and-reporting-financial-abuse.jsp (last visited Feb. 8, 2016).

[67] Letter from Benjamin M. Lawsky, Superintendent Fin. Serv. N.Y., to Financial Institutions Doing Business in the State of New York (Feb. 26, 2016), http://www.dfs.ny.gov/about/letters/ltr150226_elder_exploit_prevent.pdf.

3.4.5 Understand the roles of first responders and what cases/actions they will and will not take

Adult Protective Services

Adult Protective Services are social services programs provided by states nationwide, serving older adults and adults with disabilities who are in need of assistance.[68] APS is a generic term, not necessarily the name of the agency in each state.[69] The National Adult Protective Services Association website provides contact information for reporting suspected abuse to APS in every state.[70]

APS workers evaluate two things before opening an investigation:

- Whether the alleged victim is eligible for protective services, and
- Whether the information reported meets the legal definition of abuse, neglect or exploitation in their state or locality.

Eligibility. State law specifies which adults are eligible for protective services. In some states, APS will investigate alleged abuse of adults aged 18 or older who are vulnerable due to a physical or mental impairment. In other states, the alleged victim must be over a certain age, e.g., 60 or 65, to qualify, regardless of disability. Most states have both an age criterion and a condition criterion (e.g., physical or mental impairment, dementia, etc.) and an individual must meet both criteria to be eligible for services.

---

[68] For a description of what APS is and how it works, *see* HHS, Nat'l Center on Elder Abuse, http://www.ncea.acl.gov/Stop_Abuse/Partners/APS/How_APS_Works.aspx (last visited Feb. 17, 2016).

[69] A few states (e.g., MA and IL) have two separate agencies, one for people over age 60 or 65 and another for people from age 18 to age 60 or 65. *See* NAPSA, Get Help, http://www.napsa-now.org/get-help/help-in-your-area/ (last visited Feb. 8, 2016).

[70] NAPSA, Get Help, http://www.napsa-now.org/get-help/help-in-your-area/ (last visited Feb. 8, 2016).

Definition of mistreatment. APS workers look at whether the allegations in a given case meet the state's definition of financial exploitation, which is generally found in the state's APS statute.

Generally, if the allegations meet both the eligibility test and the definition of mistreatment test, APS may open an investigation. If APS then finds that the person has experienced or is at risk of experiencing financial exploitation, APS can decide what services, if any, are necessary for the vulnerable adult's safety or well-being and recommend a service plan. APS can also cross-report to law enforcement for criminal investigation and possible prosecution.

Law Enforcement

Financial exploitation may violate an array of criminal laws. Some states have enacted laws making elder financial exploitation a crime. But generally law enforcement personnel investigate and prosecutors charge people with other crimes such as theft, larceny, embezzlement, forgery, fraud and money laundering.[71]

Increasingly, across the country, law enforcement officers, financial crimes investigators, and prosecutors are trained on elder abuse and how to use criminal and civil laws to prosecute abusers and obtain restitution for victims.[72] Some localities have specialized units within local law enforcement agencies or prosecutors' offices with particular expertise in handling elder abuse cases.

---

[71] CFPB, *Protecting residents from financial exploitation: A manual for assisted living and nursing facilities* (May 2014), *available at* http://files.consumerfinance.gov/f/201406_cfpb_guide_protecting-residents-from-financial-exploitation.pdf; Lori Stiegel, *An Overview of Elder Financial Exploitation*, Generations: J. Am. Soc. Aging 77, 73-80 (2012).

[72] HHS, Nat'l Center on Elder Abuse, Frequently Asked Questions, http://www.ncea.acl.gov/faq/index.aspx (last visited Feb. 8. 2016).

Long-term Care Ombudsmen

Ombudsmen are advocates for residents of nursing facilities, board and care homes, assisted living facilities and similar adult care facilities, in programs administered by the Administration on Aging/Administration for Community Living. Ombudsman staff and volunteers work to resolve problems and concerns of individual residents. Every state has an Office of the State Long-Term Care Ombudsman headed by a full-time state ombudsman.[73]

Reports to state and local authorities should include core components that support the allegation and assist the responder in initiating an investigation. Reports should include facts that support and illustrate the suspicious activity in question. State law may list the things to include in the report.[74] Here are some basic components that should be included in a report to any of the authorities described above (at 3.4.5):

- The time and date of the report
- The name, address, email address and telephone number of the person reporting
- The financial institution's name and the reporter's name, title, and contact information
- the time, date, and location of the incident(s)

---

[73] CFPB, *Protecting residents from financial exploitation, A manual for assisted living and nursing facilities* (May 2014), *available at* http://files.consumerfinance.gov/f/201406_cfpb_guide_protecting-residents-from-financial-exploitation.pdf.

[74] Some states have reporting forms on their APS websites specifically for financial institution reports, e.g., CA Health and Human Services, SOC 342 at http://www.cdss.ca.gov/cdssweb/entres/forms/English/soc342.pdf. Some jurisdictions have model reporting forms. *See*, e.g., MD's Project Safe, *Model Reference Manual for Financial Institution Employees*, 2nd ed. (Rev. Sept. 10, 2013), *available at* http://www.oag.state.md.us/Consumer/ModelEmployeeReferenceManual.pdf. Many states have APS reporting forms that financial institutions may use but that are not specifically designed for financial institutions, e.g., ME Aging & Disability Servs., *Report Abuse, Neglect or Exploitation in Maine*, http://www.maine.gov/dhhs/oads/aps-guardianship/report.html (last visited Feb. 12, 2016).

- The name(s) of the persons involved, including but not limited to the alleged victim, alleged perpetrator(s) and witness(es)
- Whether the financial institution believes there is a risk of imminent danger to the alleged victim and/or to investigators/responders
- A description of the suspected financial exploitation and signs of any other type of abuse or neglect
- Statements made by the alleged victim or suspect
- Targeted deposit or other financial account(s)
- The alleged victim's disability and/or health condition including any information on cognitive status
- The relationship of the alleged perpetrator to the alleged victim, if known
- Whether a report has been made to any other public agency, and
- Whether the financial institution has conducted an internal investigation and the contact information for the individual(s) responsible for the investigation.

The CFPB recommends ascertaining the state requirements and procedures for taking oral and written reports. Consider making an oral report as soon as possible, followed by submission of a written report.

3.4.6 Expedite responses when APS, law enforcement, and other government entities investigate reports of financial exploitation and request documentation, in accordance with relevant laws

Once APS or law enforcement open an investigation, they are likely to seek records and documentation from financial institutions. It is critically important to provide information in a timely manner while complying with privacy laws.

In interviews conducted for a 2012 GAO report, APS officials in four states—California, Illinois, New York and Pennsylvania—reported that "they are often denied access on the basis of federal privacy laws or the bank's policies."[75] A 2014 survey of APS workers found that over half frequently had difficulty obtaining records necessary for an investigation from financial institutions. Almost 70 percent reported that banks required a subpoena before providing the records.[76]

The CFPB recommends that financial institutions work with their legal counsel to timely provide information when requested by APS, law enforcement or other agencies while also complying with privacy laws. The Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults noted that one of the exceptions to the GLBA notice and opt-out requirement is to "comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by federal, state, or local authorities."[77]

---

[75] GAO, Elder Justice, National Strategy Needed, supra at 34.

[76] A summary of the survey results can be found at NAPSA, *APS Professionals Speak Out About Working With Banks*, http://victimsofcrime.org/docs/default-source/financial-fraud/bank-survey-and-research-overviews-nov-2014.pdf?sfvrsn=2 (last visited Feb. 8, 2016).

[77] *Interagency Guidance on Privacy Laws, supra*; 12 CFR § 1016.15(a)(7)(ii). A state's privacy laws may be relevant to reporting elder financial exploitation to state and local authorities if the state law provision affords a consumer

Providing records in a timely manner is essential. Frequently perpetrators of elder financial abuse engage in ongoing financial exploitation, so delays may cause greater loss to older adults while an investigation is in process.

FinCEN Guidance dated June 13, 2007 clarifies that financial institutions must provide SAR supporting documentation when requested by appropriate law enforcement or supervisory agencies.[78] Service of legal process (such as a subpoena or court order) is not required when appropriate supervisory agencies and appropriate law enforcement request a copy of a SAR or supporting documentation underlying a SAR.[79] The Guidance also states that "[d]isclosure of SARs to appropriate law enforcement and supervisory agencies is protected by the safe harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions."[80]

For records requests not involving SAR supporting documentation, the CFPB recommends that financial institutions provide documents to investigatory agencies at no charge. (According to the APS survey mentioned above, many financial institutions already do so).

3.4.7 Understand constraints of first responders

Reporting suspected financial exploitation and providing supporting documentation are critical. However, financial institutions should be aware that not all reports will result in concrete action

---

greater protection than the Gramm-Leach-Bliley Act's privacy provisions and those of its implementing regulations.

78 FinCen, FIN-2007-G003, Suspicious Activity Report Supporting Documentation (June 13, 2007), *available at* https://www.fincen.gov/statutes_regs/guidance/pdf/Supporting_Documentation_Guidance.pdf. The guidance sets forth what constitutes "supporting documentation" under SAR regulations, and that financial institutions should have procedures in place for verifying that the requester is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency.

79 Id.

80 Id.

by APS, law enforcement, and other entities. Responders may not have the capacity to respond to all reports; GAO found that APS agencies lack financial resources and that these financing challenges impede APS's ability to respond to elder abuse.[81] Account holders may turn out to be ineligible for services or may refuse services. Law enforcement may prioritize other crimes.

In addition, in some cases, agencies will not be able to provide follow-up information to financial institutions due to confidentiality laws or rules. It may appear that APS or another agency did not respond or offer services when in fact the agency did act, but is not free to reveal the nature of its action.

3.5 Protect older account holders from financial exploitation

3.5.1 Comply with the Electronic Fund Transfer Act (EFTA) and Regulation E

Sometimes older account holders experience financial exploitation involving unauthorized electronic fund transfers (EFTs) from their account. Older consumers have submitted complaints to the Bureau about discovering unauthorized EFTs, such as the use of a debit card

[81] GAO, Report to the Chairman, Senate Special Comm. On Aging, *Elder Justice, Stronger Federal Leadership Could Enhance National Response to Elder Abuse* (Mar. 2011), *available at* http://www.gao.gov/assets/320/316224.pdf.

by a trusted person.[82] EFTA, implemented by Regulation E, offers important protections to these consumers.[83]

EFTA and Regulation E provide consumers with important rights when, among other things, unauthorized EFTs are made from covered accounts. This subsection summarizes some of the requirements of EFTA and Regulation E that are most relevant to unauthorized EFTs and highlights complaints that the CFPB has received.

EFTA and Regulation E provide a basic framework that establishes the rights, liabilities, and responsibilities of participants in EFT systems.[84] EFTs are defined broadly and generally include any transfer of funds initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit, or credit a consumer's account.[85]

An EFT generally is considered unauthorized if it is initiated by a person other than the consumer who has no actual authority to initiate it and if the consumer receives no benefit from it.[86] However, a transfer may be authorized if a consumer gives another person an access device such as a debit card or PIN. If a consumer gives another person a card, PIN, or other access device and authorizes that person to make transfers, the consumer is fully liable for the transfers made by that person, even if that person makes more or different transfers than the consumer

---

[82] Consumer complaints are submissions that express dissatisfaction with, or communicate suspicion of wrongful conduct by, an identifiable entity related to a consumer's personal experience with a financial product or service.

[83] Regulation E also provides protections to consumers who send remittance transfers to other consumers or businesses in a foreign country. 12 CFR §1005.33(a).

[84] *See* 15 U.S.C. § 1693 *et seq.*, and 12 CFR Part 1005.

[85] *See* 15 U.S.C. § 1693a(7); 12 CFR § 1005.3(b).

[86] 15 U.S.C. § 1693a(12); 12 CFR § 1005.2(m).

authorized, unless the consumer has notified the financial institution that transfers by that person are no longer authorized.[87]

Generally, under EFTA and Regulation E, the consumer has no liability for a timely reported unauthorized transfer and limited liability when the unauthorized transfer involves a lost or stolen access device.[88]

Follow rules for extending time limits for consumers for extenuating circumstances

Regulation E specifies that if a consumer's delay in notifying a financial institution with respect to an unauthorized EFT was due to extenuating circumstances, such as extended travel or hospitalization, the time periods for notification (as specified in the Regulation) must be extended to a reasonable time.[89] The necessity for extending time may occur with greater frequency for older consumers than for younger consumers due to the increased incidence of hospitalization among the older population. The older population (65 and over) has the highest hospitalization rate in the United States.[90]

Follow rules for accepting notices of unauthorized EFTs

Older consumers have submitted complaints to the Bureau stating that they encountered difficulties when they tried to report unauthorized transactions. For instance, older consumers submitted complaints stating that their financial institution required them to submit a police report or file a legal action as a condition of the financial institution investigating the claim.

---

[87] 15 U.S.C. § 1693a(12); 12 CFR § 1005.2(m) and comment 1005.2(m)-2.

[88] 12 CFR §§ 1005.6 and 1005.11.

[89] 12 CFR § 1005.6(b)(4) and comment 1005.6(b)(4)-1.

[90] CDC, FastStats, *National Hospital Discharge Survey: 2010 table, Number and rate of hospital discharges, available at* http://www.cdc.gov/nchs/fastats/hospital.htm.

METHOD OF GIVING NOTICE

Regulation E provides that a consumer may notify a financial institution of an unauthorized transaction in person, by telephone, or in writing.[91] Notice is given to a financial institution when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information.[92]

WHO PROVIDES NOTICE

Regulation E provides that a person acting on the consumer's behalf may give the required notice to the financial institution. As explained in the Official Interpretation, "For example, if a consumer is hospitalized and unable to report the loss or theft of an access device, notice is considered given when someone acting on the consumer's behalf notifies the bank of the loss or theft."[93] For reasons explained above, older consumers, more than their younger counterparts, may use a surrogate to notify their financial institution.

SPECIFICITY OF NOTICE

Regulation E provides that notice of an unauthorized EFT is given even when the consumer is unable to provide the account number or the card number in reporting an unauthorized transfer, as long as the consumer otherwise identifies sufficiently the account in question.[94] "For example,

---

[91] 12 CFR § 1005.6(b)(5)(ii).

[92] 12 CFR § 1005.6(b)(5)(i).

[93] 12 CFR § 1005.6(b)(5) and comment 1005.6(b)(5)-2.

[94] 12 CFR § 1005.6(b)(5) and comment 1005.6(b)(5)-3.

the consumer may identify the account by the name on the account and the type of account in question."[95]

Separately, Regulation E's proceedures for resolving errors, which include, among other things, unauthorized electronic fund transfers, provide that financial institutions may require consumers to give notice of an error only at a specified telephone number or address, but must have reasonable procedures to refer a consumer to that number or address if the consumer attempts to give notice of an error in a different manner.[96]

Once a consumer provides notice of an error, financial institutions should bear in mind their obligations under Regulation E to commence investigations, provide provisional credits, report results of investigations to consumers, and correct errors within specified timeframes.[97] A financial institution may request that a consumer provide a written, signed statement related to an error within 10 business days of an oral notice and may refrain from provisionally crediting a consumer's account if such confirmation is not received.[98] However, financial institutions may not delay beginning or completing an investigation because the consumer fails to provide the requested written confirmation.[99] Likewise, a financial institution must conduct a timely investigation whether or not a consumer provides any additional information or evidence (for example, a police report) that the financial institution has requested.[100] Financial institutions should bear in mind that EFTA provides that, in any action which involves a consumer's liability for an unauthorized EFT, the burden of proof is on the financial institution to show that the EFT

---

[95] Id.

[96] 12 CFR part 1005, comment 1005.11(b)(1)-6.

[97] 15 U.S.C. § 1693f; 12 CFR § 1005.11.

[98] 15 U.S.C. § 1693f (a); 12 CFR § 1005.11(b)(2).

[99] 12 CFR § 1005.11(c) and comment 1005.11(c)-2.

[100] *See* 15 U.S.C. § 1693f(1); 12 CFR § 1005.11(b)(1).

was authorized or, if the EFT was unauthorized, that the institution has satisfied the conditions for imposing liability on the consumer.[101]

A consumer's negligence cannot be used as the basis for imposing greater liability than is permissible under Regulation E

Older consumers may experience cognitive challenges that make remembering PINs and passwords difficult, and these challenges may prompt them to note PINs on or near a debit card. Regulation E does not permit consideration of these facts in determining the extent of the consumer's liability for an unauthorized EFT.

According to Regulation E, consumer behavior that may constitute negligence under state law, "such as writing the PIN on a debit card or on a piece of paper kept with the card," cannot be used as the basis for imposing greater liability for an unauthorized EFT than allowed by Regulation E.[102]

Similarly, "no agreement between the consumer and an institution may impose greater liability on the consumer."[103]

---

[101] 15 U.S.C. § 1693g(b).

[102] 12 CFR § 1005.6(b) and comment 1005.6(b)-2.

[103] 12 CFR § 1005.6(b) and comment 1005.6(b)-3.

3.5.2 Offer account holders the opportunity to consent to disclosure of account information to trusted third parties when the financial institution suspects financial exploitation

In addition to reporting suspected financial exploitation to law enforcement and other relevant agencies, financial institutions can protect account holders from financial exploitation by obtaining advance consent from them to inform a trusted third party that the financial institution suspects that financial exploitation has occurred, is occurring, has been attempted or will be attempted. Notifying a relative, friend or other trusted person designated by the consumer can trigger helpful protective actions and interactions.

For example, an older person might seek to withdraw a large sum of money and tell the financial institution employee that she has won the lottery and needs to pay taxes and fees up front to collect her winnings. If notified, the older person's daughter might:

- Be successful at convincing the older person that a scammer has targeted her and she should not withdraw and send the funds
- Bring together family members to develop response strategies to protect the older person from predators, and/or
- Take protective action such as filing for guardianship if the older person has diminished capacity to handle finances.

Similarly, a financial institution might detect ATM withdrawals late at night. The financial institution might be aware that an account holder resides in an assisted living facility and has limited mobility. The financial institution might contact the account holder and, depending on the response, the trusted contact person who might:

- Investigate whether home health aides or others have access to the account holder's ATM card and limit that access
- Ascertain and notify the financial institution that the transaction is unauthorized.

The CFPB recommends that financial institutions consider establishing procedures for enabling consumers to provide advance consent to sharing nonpublic personal account information with a designated trusted third party when the financial institution reasonably suspects that financial

exploitation has occurred, is occurring, has been attempted, or will be attempted. The financial institution should keep in mind factors described below that inform the design of these procedures.

GLBA generally provides that a financial institution may not disclose any nonpublic personal information about a consumer to any nonaffiliated third party unless the financial institution first provides the consumer with a notice that describes the disclosure and provides a reasonable opportunity to opt out of the disclosure, and the consumer does not opt out. GLBA permits disclosure of nonpublic personal information with the consent of the consumer, however.[104] The financial institution may obtain this consent in advance before the financial institution suspects that elder financial exploitation is occurring, has occurred, has been attempted or will be attempted.

In addition to ensuring compliance with GLBA, financial institutions may consider taking the following steps to provide consumers with the opportunity to consent to information sharing with trusted third parties.

- Establish a procedure for offering consumers the opportunity to consent—at account opening and periodically thereafter—to share account and account-related information with specified third parties under specified circumstances which may include when the financial institution reasonably suspects that financial exploitation has occurred, is occurring, has been attempted, or will be attempted.

  In determining when to communicate with account holders about providing consent to communicate with a trusted contact and identifying a trusted contact person, consider whether to designate a specific time interval (e.g., every year, every three years) or whether to tie the communication to particular events (e.g., the consumer adds an

[104] There are other exceptions to the notice and opt out provisions that permit financial institutions to report suspected financial exploitation. *See supra* at 3.4.4.

additional owner to the account, the consumer shares information about a power of attorney or a trust, the consumer has been the victim of financial exploitation) or both.

Consider which type of financial institution employee is best qualified to discuss the consent with the consumer (e.g., staff member who receives more intensive training on elder financial exploitation and/or communication skills). The CFPB recommends developing an explanatory script or talking points in plain language for staff members to use when offering consumers the opportunity to execute the consent and walking them through the consent form.

- Develop a consent form in plain language to enhance consumer understanding. Before implementing the consent form, consider testing the form to ensure consumer understanding. Financial institutions might include in this consent form:
  - A description of the triggers for sharing information with the trusted contact or multiple trusted contacts
  - A statement that, notwithstanding the consumer's consent, the financial institution will not disclose nonpublic personal information to a designated third party if the financial institution reasonably believes that the third party has engaged in, is engaging in, or will engage in financial exploitation of the consumer
  - An acknowledgment that the consumer has a right to revoke the consent and/or execute a new consent naming a different trusted third party.

Note that an account holder with a cognitive impairment may lack capacity to consent to information sharing with a trusted third party and/or to revoke a prior consent.

There may be relevant state privacy laws and other statutes that impact the consumer's ability to consent to sharing information with trusted third parties, the form of the consent or other aspects of this recommendation.

3.5.3 Consider sharing information with persons acting in a fiduciary or representative capacity when the financial institution suspects financial abuse, regardless of whether the consumer has consented to share information with that person

GLBA permits financial institutions to share nonpublic personal information with "persons acting in a fiduciary or representative capacity on behalf of the consumer" without providing the consumer with notice and an opportunity to opt out.[105] Financial institutions may share information with these third parties without obtaining the consumer's consent.

3.5.4 Offer age-friendly services to older consumers that can enhance protections against financial exploitation

Financial institutions can provide information and services to consumers, including older consumers, which can enhance protections against financial exploitation. These services include:

Provide information about planning for incapacity and disability

Advance planning for the possibility of diminished capacity, illness and disability can protect older adults from financial exploitation. For example, naming a trusted person to serve as an agent under a power of attorney or other fiduciary increases the odds that the person managing finances will act in the best interests of the account holder. Also, the fiduciary can protect the account holder from predators and can monitor transactions.

[105] 12 CFR § 1016.15(a)(2)(v).

The CFPB offers two helpful free resources that relate to advance planning. A Consumer Advisory called **Planning for Diminished Capacity and Illness**, issued jointly by the CFPB and the Securities and Exchange Commission, can help both the older adult and trusted third parties who assist the older person with finances. *See* http://files.consumerfinance.gov/f/201505_cfpb_consumer-advisory-and-investor-bulletin-planning-for-diminished-capacity-and-illness.pdf. In addition, the CFPB's **Managing Someone Else's Money** guides are for family members and friends serving as fiduciaries for an adult who cannot manage money and property. These guides can also be useful for older account holders who are doing advance planning, because they explain the duties of fiduciaries and also raise awareness about financial exploitation and scams. Older account holders can share them with the person they name as a fiduciary. A number of banks and credit unions have ordered these guides in bulk, have distributed them to employees, or have shared them on their websites. *See* www.consumerfinance.gov/managing-someone-elses-money.

Honor powers of attorney

A financial power of attorney (POA) is an important advance-planning tool because it enables consumers to designate a fiduciary who can act on the consumer's behalf if the consumer is cognitively impaired or otherwise unable to handle financial matters independently. Generally POAs created to plan for the future are durable and remain in effect even if the maker loses capacity.[106]

[106] By 1984, all states and the District of Columbia had enacted provisions of the Uniform Durable Power of Attorney Act enabling people to create durable powers of attorney. Karen E. Boxx, *The Durable Power of Attorney's Place in the Family of Fiduciary Relationships*, 36 Ga. L. Rev. 1, 9 (2001). The Uniform Power of Attorney Act, adopted by

While the POA is an important tool, it provides opportunities for the agent to financially exploit an incapacitated individual.[107] Financial institution employees should be aware that older account holders may be targets of power of attorney abuse.

Consumers and elder law attorneys report that financial institutions sometimes refuse to accept a POA for reasons unsupported by state law, such as the POA was not on the financial institution's preferred form[108] or was not executed within a given period of time.[109] In 2002 the Uniform Law Commission found that sixty-three percent of surveyed attorneys indicated that they had experienced difficulty obtaining third party acceptance of an agent's authority and seventeen percent indicated that it was a frequent problem.[110]

---

the Uniform Law Commission in 2006, defines a power of attorney as durable unless otherwise indicated by the maker. Uniform Power of Attorney Act § 104 (2006), http://www.uniformlaws.org/shared/docs/power%20of%20attorney/UPOAA_2011_Final%20Act_2014sep9.pdf.

[107] Lori A. Stiegel & Ellen V. Klem, AARP, *Power of Attorney Abuse: What States Can Do About It* 5 (2008). *See also* Linda S. Whitton, National Conference of Commissioners on Uniform State Laws, *National Durable Power of Attorney Survey Results and Analysis* (2002), *available at* http://www.uniformlaws.org/shared/docs/power%20of%20attorney/dpasurveyreport_102902.pdf.

[108] Under Florida law, "[a] third person may not require an additional or different form of power of attorney for authority granted in the power of attorney presented." Fla. Stat. § 709.2120(2).

[109] *See*, e.g., *When Third Parties Refuse to Honor a Power of Attorney*, http://dennisfordhamlaw.com/when-third-parties-refuse-to-honor-a-power-of-attorney/ (last visited Feb. 17, 2016); Can banks legally refuse to accept a durable power of attorney?, https://www.caring.com/questions/can-banks-refuse-power-of-attorney (last visited Feb.17, 2016); Both Attorneys and Courts are Tired of Financial Institutions' Refusal to Accept Powers of Attorney (Mar. 2013), http://www.lexisnexis.com/legalnewsroom/estate-elder/b/estate-elder-blog/archive/2013/03/12/both-attorneys-and-courts-are-tired-of-financial-institutions-refusal-to-accept-powers-of-attorney.aspx (last visited Feb. 17, 2016).

[110] Linda S. Whitton, National Conference of Commissioners on Uniform State Laws, *National Durable Power of Attorney Survey Results and Analysis* (2002), *available at* http://www.uniformlaws.org/shared/docs/power%20of%20attorney/dpasurveyreport_102902.pdf; *See* also Linda S. Whitton, *The Uniform Power of Attorney Act: Striking a Balance Between Autonomy and Protection*, 1 Phoenix L. Rev. 343, 352 (2008), *available at* http://www.cobar.org/repository/Inside_Bar/Elder/2.19.09/Whitton-Phoenix_Law_Review_art_.pdf.

A financial institution's refusal to honor a valid POA can create hardships for consumers who need designated surrogates to act on their behalf. For example, a financial institution may fail to honor a POA because it is not on the bank's preferred form, but the maker of the power of attorney may now lack capacity to make a new instrument, leaving the account holder without a surrogate and thwarting his or her original plan.

Many state laws provide broad protection for financial institutions that accept powers of attorney in good faith.[111] The Uniform Power of Attorney Act (UPOAA), for example, provides protection for good faith acceptance of an "acknowledged" (e.g., notarized) power of attorney.[112]

In addition, the UPOAA provides a safe harbor for a financial institution that refuses to accept a power of attorney when, among other reasons, the third party believes that the agent lacks authority and when the third party believes that the account holder may be the victim of financial abuse by the agent.[113] If none of the safe harbor provisions apply, the UPOAA provides that a person that refuses to accept a power of attorney is subject to a court order mandating acceptance of the power of attorney and liability for attorney's fees and costs in a court proceeding.[114]

The CFPB recommends that financial institutions consider establishing procedures that will

---

[111] *See*, e.g., Cal. Prob. Code § 4303; Fla. Stat. § 709.2119(5); N.M. Stat. Ann. § 45-5B-119(C).

[112] Uniform Power of Attorney Act § 104 (2006). Seventeen states had adopted the UPOAA by February, 2016. *See* http://www.uniformlaws.org/Act.aspx?title=Power%20of%20Attorney. States have adopted the full UPOAA or parts of it.

[113] Uniform Power of Attorney Act § 120(b), Alternative A and § 120(c) Alternative B (2006). In the latter situation, either the third party or someone else must make a report to the local APS office in order for the safe harbor to take effect.

[114] Uniform Power of Attorney Act § 120(c), Alternative A and § 120(d), Alternative B. *See* also similar state law provisions, e.g., Alaska Stat. § 13.26.353(c); Minn. Stat. Ann. § 523.20; N.Y. Gen. Oblig. Law § 5-1504.

- Enable the institution to make prompt decisions on whether to accept a power of attorney when presented
- Ensure that decisions are made by staff qualified to assess the document based only on state law and other appropriate considerations, and
- Enable frontline staff to recognize red flags for power of attorney abuse and alert qualified staff who may determine whether the institution should refuse to honor the document and make a report to relevant authorities.

Offer protective opt-in account features

Financial institutions can provide enhanced protection against the risk of elder financial exploitation by offering consumers selective account options. Opt-in account restrictions and alerts allow account holders to take preventive measures against exploitation risk. Financial institutions can offer restrictions, alerts, and other features responsive to account holder concerns and preferences.

Examples of account opt-in features that could reduce the risk of elder financial exploitation include, but are not limited to:

- Cash withdrawal limits
- Geographic transaction limits
- Transaction restrictions for specified merchants or merchant categories
- Alerts for specified account activity
- Alerts to authorized third parties, and
- Read-only access to accounts for authorized third parties.

Opt-in features may benefit financial institutions through increased public association with account security and their demonstrated commitment to the protection of vulnerable customers.

Financial institutions can offer view-only access to trusted third parties designated by the account holder. For example, a third-party monitoring feature can enable a designated family member or friend to monitor an account for irregularities without having access to funds or the

ability to make transactions. The third party monitors the account through online banking or duplicate monthly statements.[115]

Offer convenience accounts as an alternative to traditional joint accounts

Some older adults need help with financial accounts and often open traditional joint bank accounts to enable a family member or other helper to pay bills and assist with other transactions. There are several risks or unintended consequences associated with joint accounts:

- The joint owner can withdraw money for his or her own use or mismanage the older account holder's money
- Creditors of the joint owner may use legal processes to try to satisfy their debts from the money in the account
- When the older person dies, depending on the terms of the account and state law, money in the joint account may be distributed by the bank to the friend or family member whose name is on the account, possibly subverting the intended estate plan when there are multiple heirs.

The CFPB recommends that financial institutions routinely provide educational information to consumers about the consequences of opening traditional joint accounts.[116] Financial

---

[115] Jilenne Gunther, AARP, *Bank Safe: A Comprehensive Approach to Better Serving and Protecting Consumers*, (2016), *available at* http://www.aarp.org/content/dam/aarp/ppi/2016-02/banksafe-initiative-aarp-ppi.pdf; Jilenne Gunther & Robert Neill, *Innovative Case Examples of: Banking Safe* (2016), *available at* http://www.aarp.org/content/dam/aarp/ppi/2016-02/innovative-case-examples-of-banking-safe-ppi.pdf.

[116] The CFPB's *Ask CFPB* online consumer education tool provides plain-language information on this topic. *See* Ask CFPB, http://www.consumerfinance.gov/askcfpb/1145/i-would-be-able-have-my-friend-or-family-member-help-my-bill-paying-and-banking-what-are-my-options.html (last updated on Oct. 11, 2013). The American Bankers Association Foundation and AARP have created an infographic about whether a joint bank account is right for a consumer. *See* AARP & ABA Foundation, *Look Before You Leap*, https://www.aba.com/Engagement/Documents/ABAAARPJointAccounts.pdf (last visited Feb. 8, 2016).

institutions also should provide this education when an older consumer requests changing an existing account to a joint account.

Multi-party accounts without right of survivorship, also known as convenience accounts or agency accounts, may be good alternatives to traditional joint bank accounts.[117] When set up properly under applicable state law, the helper added to the account can make deposits and withdrawals on the account and legally must use the account only for the benefit of the owner in accordance with the owner's wishes.[118] When the owner dies, the account is conveyed according to the individual's will. The CFPB recommends that financial institutions routinely offer such convenience accounts as an alternative to traditional joint bank accounts. Financial institutions should train employees on how to explain the different types of accounts to consumers and ensure that convenience accounts are properly opened.

Consider educating consumers about avoiding fraudulent transfers

Specific information or warnings about electronic fund transfers may help older account holders avoid fraudulent transactions. For example, if consumers are adding authorized users or providing another person with an access device, consider alerting them at the time of the request to potential pitfalls of allowing another person to have access to their account, particularly regarding their liability for unauthorized transactions by someone who was given an access device or PIN. In addition, consider alerting them to the dangers of writing a PIN on or near a debit card.

---

[117] Charles P. Sabatino, *Damage Prevention and Control for Financial Incapacity*, 305 JAMA (Feb. 16, 2011), *available at* http://jama.jamanetwork.com/article.aspx?articleid=645586&resultclick=1.

[118] Id.

3.6 Collaborate with other stakeholders

Numerous organizations on the local, regional and state level often play a critical role in preventing, detecting, and responding to elder financial exploitation.[119] These organizations may also provide support to victims, and work on broad-based strategies to combat elder financial exploitation.

Across the U.S., organizations are collaborating in an effort to improve coordination among the entities working with and protecting elders.[120] These collaborations take on a variety of forms. In some communities, groups of professionals meet regularly to review cases of financial exploitation. Some groups conduct community education activities and trainings for professionals, older adults, family members, aging service providers, and the community at large.

In many communities, financial institutions participate in these efforts and the CFPB recommends that they do so.

3.6.1 Work with law enforcement and APS

Financial institutions should take specific steps to develop collaborative relationships with law enforcement and adult protective service responders, such as:

- Coordinating with law enforcement and APS to share information about each organization's policies and procedures for detecting, assessing, and reporting cases.

---

[119] These entities include, among others, APS, law enforcement, legal services programs, aging network organizations, aging services providers and other non-profits.

[120] Shelly L. Jackson & Thomas L. Hafemeister, Pure Financial Exploitation vs. Hybrid Financial Exploitation Co-Occurring With Physical Abuse and/or Neglect of Elderly Persons, 2 Psychol. of Violence 285 (2012), *available at* http://psycnet.apa.org/psycinfo/2012-04350-001/ (available with subscription).

- Working with law enforcement and APS to identify training needs and develop strategies and protocols for sharing information, and responding to suspicious activities. For example, developing local and regional relationships with relevant personnel at law enforcement and protective service agencies can facilitate timely response to reports and ensure that staff has appropriate points of contact when questions or roadblocks arise.
- Providing expert consultation on banking and finance documents, processes and procedures to assist law enforcement and adult protective services with their case investigations, when requested.

3.6.2 Participate in and support coordinated efforts to educate older account holders, caregivers and the general public about elder financial exploitation

The CFPB recommends that financial institutions collaborate with state and local agencies and senior service organizations by offering educational programs and distributing resource materials to older account holders, family members, caregivers, and the community at large. Many local aging departments, state regulators, councils on aging, senior centers, and faith-based organizations are already engaged in these efforts.[121]

[121] The CFPB provides resources and materials for consumer education. Money Smart for Older Adults-Prevent Elder Financial Exploitation (MSOA) is an awareness program, produced by the CFPB and the Federal Deposit Insurance Corporation (FDIC), that utilizes a train-the-trainer model. Financial institutions can collaborate with local stakeholders to offer community education and awareness seminars and workshops. Also, financial institutions may consider hosting a train-the-trainer session to initiate the development of a local or regional MSOA speaker's bureau. The program is available in English and Spanish. Financial institutions can download the training module at www.fdic.gov/moneysmart and order the participant/resource guide at www.promotions.usa.gov/cfpbpubs.html. The Managing Someone Else's Money guides, discussed above *supra* at 3.5.4, are useful for distribution by financial institutions at educational events, as family members of older consumers often manage money and property for them as they age. Financial institutions can order the guides for free and in bulk at www.promotions.usa.gov/cfpbpubs.html#someone.

3.6.3 Participate in and support local or regional multidisciplinary network initiatives

In various locations around the country, key stakeholders convene as multidisciplinary networks to address the problem of elder abuse including financial exploitation. Members of these groups can include APS agencies, aging service agencies, law enforcement representatives, legal services organizations, non-profit senior service providers and financial services providers. These networks engage in activities such as education, training and individual case review. For example, Triads are community groups in which local law enforcement, aging service providers, and the community work together to prevent crime against older adults. Financial institutions may identify opportunities to engage in local multidisciplinary networks focusing on elder financial exploitation.

Some of these networks work together to provide expert advice to APS and law enforcement to support the investigation or processing of complex cases. These case review groups are often referred to as multi-disciplinary teams (MDTs) or financial abuse specialist teams (FASTs) but they may adopt another name that reflects their geographic location or the unique organizational structure of their group. Across the nation, there are a limited number of multidisciplinary teams with a case consultation function. Those teams most often work in metropolitan areas.

Financial institution personnel can be valuable members and contributors to "networks" as they engage in both educational and case review functions. They can provide expertise as speakers for community groups and as experts in finance who can assist investigators by identifying and analyzing documents that are important to the investigation. Financial institution representatives also can educate responders and investigators on the nuances of banking policy and procedures to enhance mutual understanding and cooperation in the investigative process. Conversely, adult protective services and law enforcement can be good sources of information, resources for training financial institution staff, and co-presenters at consumer and industry events. Some multidisciplinary teams limit discussions of specific cases to government agencies working on the case, but even in those situations financial institution personnel can offer and provide valuable ad-hoc support.

Financial institutions may be able to identify multidisciplinary networks in their area by contacting the local Area Agency on Aging (AAA), APS agency, or senior information and referral hotline. The Eldercare Locator, supported by the US Department of Health and Human

Services, enables users to search for their local AAA and APS agency and is accessible at www.eldercare.gov.

4. Conclusion

Financial institutions have a tremendous opportunity to serve older consumers by vigorously protecting them from financial exploitation. The CFPB offers the above recommendations to assist financial institutions in their efforts to protect older account holders from financial exploitation. Interviews with many individual financial institutions, trade associations, prosecutors, aging services providers and other stakeholders informed the CFPB's recommendations. The CFPB found that numerous financial institutions nationwide already have implemented many of the recommendations included in the Advisory, or are considering ways to best serve their older account holders. The Bureau looks forward to continuing to work with financial institutions and seeing a broad spectrum of financial institutions implement its recommendations so that a greater number of older Americans can enjoy later life economic security.

APPENDIX A:

Warning signs that may indicate elder financial exploitation

A variety of behaviors and account activities may signal that a consumer is at risk of or is the victim of elder financial exploitation. These warning signs are not proof of financial exploitation; rather, they are signs that should trigger investigation and other proactive activities described in this report. Proactive steps are especially important if staff members detect more than one red flag. Due to the evolving nature of fraud and the methods by which exploitation is perpetrated, the CFPB encourages financial institutions to maintain an up-to-date list of behaviors and activities that indicate fraud risk for older consumers. The CFPB compiled the following list of risk indicators from several sources.[122]

---

[122] *See* BITS Financial Services Roundtable, *Protecting the Elderly and Vulnerable from Financial Fraud and Exploitation* at 11-13 (Apr. 2010), *available at* http://fsroundtable.org/wp-content/uploads/2015/05/BITSProtectingVulnerableAdults0410.pdf; BITS Financial Services Roundtable, At-Risk Adult Training Curriculum (Feb. 2013), *available at* http://fsroundtable.org/wp-content/uploads/2015/09/BITS-Roundtable-At-Risk-Adult-Training-Curriculum-Jan-2013.pdf; Presentation, Coalition for Elder Justice in Connecticut, *Preventing Elder Financial Exploitation: The Role of Financial Institutions in Connecticut* (2015), *available at* http://coa.cga.ct.gov/images/pdf/financialabuse/ElderJusiticeFinancialInstitutionsTraining2.12.15.pdf; FIN-2011-A003, *Advisory to Financial Institutions, supra*.

Interactions with older consumers, caregivers and other third parties

1. A previously uninvolved relative, caregiver or friend begins conducting financial transactions on behalf of an older consumer—or claims access or privileges to the consumer's private information—without proper documentation

2. An older consumer associates with new "friends" or strangers

3. A caregiver or other third party shows excessive interest in the older consumer's finances or accounts, does not allow the consumer to speak for him or herself, or is reluctant to leave the older consumer's side during interactions with the financial institution

4. An older consumer exhibits an unusual degree of fear, anxiety, submissiveness or deference to a caregiver or other third party

5. An older person expresses excitement over a financial opportunity, prize, or windfall

6. An older consumer lacks knowledge about his or her personal financial status or accounts, or is reluctant to discuss financial matters

7. An older consumer appears to neglect or experience a decline in appearance, grooming, or hygiene

Account activity

1. Large increases in account activity, such as daily maximum currency withdrawals from an ATM

2. Large gaps in check numbers, or "out of sync" check numbers

3. Uncharacteristic non-sufficient funds activity or overdrafts

4. Uncharacteristic debit transactions (including unusual ATM use)

5. Uncharacteristic lapses in payments for services

6. Disregard for penalties when closing accounts or certificates of deposit

7. Abrupt changes to financial documents, such as a new power of attorney, a change to a joint account or a change in account beneficiary

8. Excessive numbers of payments or payments of large sums to a caregiver or third party

9. New account use soon after adding an authorized user

10. Statements mailed to an address separate from customer's residence

11. New activity on an inactive account or joint account

12. Signatures that do not match or appear suspicious

13. Uncharacteristic requests to wire money