REPORT TO THE PRESIDENT

Independence, Technology, and Connection in Older Age

Executive Office of the President

President's Council of Advisors on Science and Technology

March 2016

REPORT TO THE PRESIDENT

Independence, Technology, and Connection in Older Age

Executive Office of the President

President's Council of Advisors on Science and Technology

March 2016

About the President's Council of Advisors on Science and Technology

The President's Council of Advisors on Science and Technology (PCAST) is an advisory group of the Nation's leading scientists and engineers, appointed by the President to augment the science and technology advice available to him from inside the White House and from cabinet departments and other Federal agencies. PCAST is consulted about, and often makes policy recommendations concerning, the full range of issues where understandings from the domains of science, technology, and innovation bear potentially on the policy choices before the President.

For more information about PCAST, see www.whitehouse.gov/ostp/pcast

How Technology Can Protect Older Adults' Economic Security

Cognitive impairment can often reduce a person's ability to manage finances ("financial capacity"). When Alzheimer's, Parkinson's, or similar diseases become symptomatic, declines in financial capacity are typically even greater.[114] Compared to younger adults, older adults may be more likely to make poor financial decisions that depend on recent learning,[115] although older adults are likely to exhibit less risk taking if a decision relies on well-learned behaviors. This may be why older adults were more likely to express intent to purchase products the Federal Trade Commission had cited as fraudulently marketed[116] or to make suboptimal decisions across financial tasks such as fee payments or credit card balance transfers.[117] Notably, these decisions often either involve interactions with technology or can be identified with technology.

Changes in financial capacity—skills, knowledge, or judgment—are among the reasons that older adults are more likely to be victims of financial fraud and exploitation. The fraud can go unnoticed for some time as reduced financial capacity is often the first effect of cognitive impairment.[118] The annual losses due to fraud and exploitation are estimated in the billions of dollars.[119] A 2010 study gauged it as $3

---

[113] The President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, 2014, See: www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[114] Marson, D.C., Sawrie, S.M., Snyder, S., McInturff, B., Stalvey, T., Boothe, A., Aldridge, T., Chatterjee, A., Harrell, L.E., "Assessing financial capacity in patients with Alzheimer's disease: a conceptual model and prototype instrument," *Archives of Neurology*, 57: 877-84, 2000; Martin, R.C., Triebel, K.L., Kennedy, R.E., Nicholas, A.P., Watts, R.L., Stover, N.P., Brandon, M., Marson, D.C., "Impaired financial abilities in Parkinson's disease patients with mild cognitive impairment and dementia," *Parkinsonism & Related Disorders,* 19: 986-90, 2013.

[115] Mata, R., Josef, A.K., Gregory R., Samanez-Larkin, G., Hertwig, R., "Age difference in risky choice: a meta-analysis." *Annals of the New York Academy of Sciences*, 1235: 18-29, 2011.

[116] Denburg, N.L., Cole, C.A., Hernandez, M., Yamada, T.H., Tranel, D., Bechara, A., Wallace, R.B., "The orbitofrontal cortex, real-world decision making, and normal aging." *Annals of the New York Academy of Sciences*, 1121: 480-498, 2007.

[117] Agarwal, S., Driscoll, J,. Gabaix, X., D. Laibson, D., "The age of reason: Financial decisions over the life cycle and implications for regulations." *Brookings Institution,* 973790: 2009. See: www.brookings.edu/~/media/Projects/BPEA/Fall%202009/2009b_bpea_agarwal.PDF

[118] Triebel, KL., Martin, R., Griffith, HR., Marceaux, J., Okonkwo, OC., Harrell, L., Clark, D., Brockington, J., Bartolucci, A., Marson, DC., "Declining financial capacity in mild cognitive impairment: A 1-year longitudinal study. Neurology," *Neurology*, 73: 928-34, 2009.

[119] MetLife Mature Market Institute "The MetLife Study of Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation Against America's Elders" www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf, 2011 and The 2015 TruLink study used measurement that accounted for the different kinds of elder abuse and estimated the total costs of all causes of abuse to be $36.48 billion.

billion a year, and a 2015 study suggested annual losses to be as high as $36 billion.[120] When these losses occur, family or public sources of funds often have to support day-to-day expenses and medical care.[121] Since older adults generally are not working, they cannot rebuild their lifetime savings after making an unsuitable financial decision or being a victim of fraud or exploitation.[122]

Exploitation and fraud manifest themselves in numerous ways.[123,124] In the grandparent scam, for example, an older adult receives a phone call from a person who pretends to be the older adult's grandchild, claims trouble that requires urgent financial help, and begs the grandparent not to tell the child's parents. The help is a cash transfer to pay a bill, fine, or bail.

Although the kinds of fraud and exploitation and their perpetrators vary, many involve an older adult transferring or withdrawing cash, which is why banks and other financial institutions should be able to identify routinely not only declines in financial capacity but also fraud and exploitation. Bank personnel could take immediate action in a face-to-face encounter, but technology for online banking could also identify unusual activity compared to the client's past behaviors and patterns. This would be the case, for example, when a client who has never used a bank card transfers money to overseas accounts or withdraws cash at an ATM. There are also technologies that could prevent or limit fraud, such as providing read-only views of accounts to caregivers or algorithms that flag potential declines in financial capacity (Box 3). While these technologies and analytics exist, the banking and financial services industries have not widely adopted them.

Multiple Federal agencies are engaged in activities to stop or prevent financial exploitation of older adults, including the Administration for Community Living, Consumer Financial Protection Bureau's (CFPB) Office for Older Americans, Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and Department of the Treasury's Financial Crimes Enforcement Network (FinCEN),

---

[120] MetLife Mature Market Institute study, and True Link studies.

[121] A Utah Division of Aging and Adult Services study used a review of 80 financial exploitation cases from 2010 to estimate that Utah seniors and businesses lost $4,766,196 and the state's Medicaid program would have to pay about $900,000 for the care of adults who suffered exploitation. Gunther, Jilenne, "The 2010 Utah Cost of Financial Exploitation," Utah Division of Aging and Adult Services, 2012. See: victimsofcrime.org/docs/default-source/financial-fraud/2011-economic-cost-of-financial-exploitation.pdf?sfvrsn=2.

[122] An example of the impact of losses in financial capacity on a patient and family is captured in "Money woes can be early clue to Alzheimer's disease," *The New York Times*, 30 October 2010, which recounts the story of Arthur Packel, whose earliest symptoms of Alzheimer's disease were troubles making financial decisions resulting in a loss of his business and much of his family's wealth in order to pay creditors. See: www.nytimes.com/2010/10/31/health/healthspecial/31finances.html?_r=0.

[123] The National Council on Aging categorizes fraud and exploitation into ten groups: Medicare and health insurance fraud, counterfeit prescription drugs, funeral and cemetery scams, fraudulent anti-aging products, telemarketing, Internet fraud, investment schemes, homeowner/reverse mortgage scams, sweepstakes and lottery scams, and the grandparent scam. www.ncoa.org/economic-security/money-management/scams-security/top-10-scams-targeting-seniors.

[124] United States Government Accountability Office. Report to Congressional Requesters. "Elder Justice: National Strategy Needed to Effectively Combat Elder Financial Exploitation," *GAO-13-110*, 2012.

and Department of Justice. Their activities include raising awareness of the problem, educating consumers and the industry, and intervening to address fraud and exploitation and impairments in financial capacity.[125] The 2009 Elder Justice Act created the Elder Justice Coordinating Council and an Advisory Board on Elder Abuse, Neglect, and Exploitation to develop priorities for the elder justice field, coordinate Federal activities, and provide recommendations to Congress.

Other groups, such as private organizations and industry groups, are focused on reducing financial fraud and exploitation.[126] A 2012 Government Accountability Office report on financial exploitation found that much of the investigation of fraud and exploitation is handled by State social services, criminal justice

Box 3. A case study in how a bank uses technology to enhance older adults' financial security

Bank of American Fork is a leader in using online, view-only accounts to promote age-friendly banking practices. They came to use this technology as part of a culture change that includes employee awareness and training and laws that mandate reporting cases of suspected fraud or abuse.

Five years ago two events occurred: the bank was approached by a customer writing a book about individuals over the age of 55 navigating their rights, and the Utah Division of Aging and Adult Services issued a study that demonstrated the cost of elder financial exploitation. The timing of these two events coincided with the company's recognition that Utah mandated that financial services report suspected elder abuse, but the bank managers had been reluctant to get involved in cases because of concern that this would reflect poorly on the bank, and even if they did, they were poorly equipped to address customers experiencing financial exploitation or impaired capacity.

Their response was multi-pronged. They developed a toolbox of banking services for elderly clients, built around products called Account*Smart* Tools for Seniors. They also engaged in public seminars for seniors and caregivers to raise awareness. Employee training includes how to recognize the signs of elder financial abuse and report it and how to help families structure banking needs to protect both the senior and the caregiver, such as recommending limited power of attorney to assist seniors and their caregivers in managing finances.

Technology is essential as well. The bank offers senior-friendly iPad applications that use intuitive design, automatic transfers and bill payments, and the innovative view-only access to accounts. "View-only" access allows a third party, such as a friend or adult child, to see a senior's account transactions but does not allow the viewer to make transactions. This account allows the third party to identify concerning transactions or changes in patterns that might signal a decline in financial capacity or abuse. The inability for the third party to make transactions protects the senior from fraud and protects the third party from unwarranted suspicion that they might commit fraud.

---

[125] United States Government Accountability Office, "National Strategy Needed to Effectively Combat Elder Financial Exploitation," *GAO-13-110*, 2012, and White House Conference on Aging, Elder Justice: See: www.whitehouseconferenceonaging.gov/blog/policy/file.axd?file=/Elder%20Justice%20Policy%20Brief/Elder%20Justice%20Policy%20Brief%205_08_15_FINAL.pdf.

[126] As examples, see: "Protect Your Money," Protect Your Money, Accessed March 14, 2016, www.aba.com/Consumers/Pages/Consumer_PYM.aspx; and "Senior Investor Protection Resource Center," Sifma, Accessed March 14, 2016, www.sifma.org/issues/savings-and-retirement/senior-investor-protection/overview/.

and consumer protections systems, and particularly the county-by-county system of Adult Protective Service (APS) agencies that are charged with investigating and substantiating cases of suspected elder fraud, abuse, or neglect.[127] The broad range of organizations highlights the need to integrate and coordinate activities.

PCAST believes that one way the Federal Government can achieve a more integrated and coordinated network is to more accurately measure the size of the problem and issue an annual report of the kinds of abuse and exploitation and their costs to the nation. The Currency and Foreign Transactions Reporting Act, commonly called the Bank Secrecy Act, provides a regulatory framework for reporting cases of fraud and exploitation into a central database. The Act requires financial institutions to report suspicious transactions, called Suspicious Activity Reports (SARs), to FinCEN at the Department of Treasury. Since 2011, institutions can mark SARs reports as incidents of elder financial exploitation, which gives the Federal Government additional data on the size, scope, and trends in elder exploitation, data that are essential for evidence-based policymaking.[128]

Beyond measurement, two technological approaches are particularly promising. Financial institutions could use algorithms to passively identify transactions that may signal impairments in financial capacity as well as fraud or exploitation. Algorithms could identify instances such as missed payments, repeated withdrawals, or transfers to atypical destinations that are indicative of a problem. These algorithms would be similar to existing ones used by large credit card issuers to detect whether a card has been lost or stolen, such as FICO's Falcon Fraud Manager Machine learning system.[129]

In addition, technologies could allow trusted parties, such as a family member or caregiver, to monitor financial accounts for impaired financial capacity or exploitation. View-only online accounts, such as

Box 4. EverSafe's use of algorithms to unobtrusively monitor activity across multiple accounts

An example of technology that unobtrusively and remotely monitors multiple financial accounts across institutions has been developed by EverSafe, a company founded in 2012 after the Founder and CEO's mother was a victim of multiple credit card scams. EverSafe's rules-based learning system developed in consultation with industry experts analyzes its members' bank, investment and credit card accounts, and credit reports on a daily basis to identify suspicious activity. Once suspicious activity is identified, an alert is sent to the member along with designated trusted advocates, such as family members, professionals, powers of attorney and guardians. These advocates have read-only access to financial information and serve as an extra set of eyes in monitoring accounts, credit reports and alerts. Read-only access means money cannot be moved, and no financial transactions can be effected through the use of EverSafe. This is a safer alternative to creating a joint account which can be subject to exploitation or the joint owner's creditors. Once alerted, EverSafe assists in remediation and tracks issues through to resolution.

---

[127] United States Government Accountability Office, "National Strategy Needed to Effectively Combat Elder Financial Exploitation," *GAO-13-110*, 2012.
[128] Department of the Treasury, Financial Crimes Enforcement Network. "Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation." FIN-2011-A003, 2011.
[129] Urban, M., *Public Comment*, 2011, See: www.federalreserve.gov/SECRS/2011/March/20110303/R-1404/R-1404_022211_67635_571427685645_1.pdf.

described in the case studies of Bank of American Fork and EverSafe (Box 4), allow a trusted person to monitor in real time the activity of another person's account without the ability to trade or manipulate assets or without revealing the balance. General purpose bank-account monitoring software has been around for some time, but technologies specific to elder abuse—for example, specialized algorithms a customer can add to an existing account, aggregation tools to bring transactions from multiple accounts into a single viewable portal, and real-time detection systems to prevent fraudulent or exploitative transactions before they occur—have only recently been introduced into the market.

There are several barriers to industry-wide adoption of new algorithms or third-party monitoring. No business model exists to foster the creation or implementation of algorithms by the banking industry itself. In addition, after a bank identifies a transaction as suspect and therefore needs to issue a SAR, financial institutions can be concerned that reporting the SAR to Adult Protective Services could violate privacy laws at both the State and Federal level. States have laws on reporting suspected cases of elder abuse, but they vary in who can report, whether reporting is encouraged or mandatory, and whether there are protections from liability for reporting and delaying a trade.[130] All the relevant Federal agencies have issued joint guidance indicating that they do not anticipate initiating enforcement action for financial institutions reporting elder abuse pursuant to State mandates,[131] but financial institutions remain concerned that taking steps to intervene on behalf of a client can violate rules on executing trades in a timely manner.

Financial institutions also noted a challenge of how to address transactions that raise a concern of impaired capacity, but not fraud or exploitation that would necessitate a SAR. As illustrated in the Bank of American Fork case study, institutions expressed a concern that bringing the transaction to the attention of the customer or even a third party the customer designated, such as an adult child or friend, or reporting to local law enforcement, could cause customer dissatisfaction and ultimately the loss of that customer.

The challenges to adopting online view-only accounts are how to make them part of routine banking practice. At the time a young or middle-aged customer is opening a bank or credit card account, he or she often does not select an institution based on the age-friendly features the customer may eventually need; in turn, banks are hesitant to raise the issue. By the time the need arises, the customer may not wish to switch accounts or may not be able to execute good judgment in the decision of how much extra financial authority should be delegated and to whom. Additionally, customers often have multiple accounts across several institutions, creating the challenge of aggregating information from multiple accounts into one secure portal.

With the entire industry facing the same problem, no one institution has the incentive to be the first to make passive monitoring and reporting and online view-only accounts part of routine practice. A

---

[130] PCAST identified three states—Delaware, Missouri, and Washington—that permit a financial institution to put a hold on a suspicious transaction while it is being investigated for fraud or exploitation.

[131] Board of Governors of the Federal Reserve System, "Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults," 1-5, 2013, See: www.fdic.gov/news/news/press/2013/Interagency-Guidance-on-Privacy-Laws-and-Reporting-Financial-Abuse-of-Older-Adults.pdf?source=govdelivery.

regulatory nudge could, we believe, overcome this barrier and make these technologies and the practices that surround them part of routine banking and financial management. Customers would expect to have these conversations as part of opening an account at an institution or in communication with an online bank to meet their needs over the long term.

To protect the finances of older adults experiencing cognitive decline, the Federal Government should encourage the banking and financial services industries to build the capability to identify declines in financial capacity, promote older adults' economic security, and protect their assets from fraud or exploitation and make the resultant information available to seniors. At minimum, the signatories to the 2013 Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults [i.e., Board of Governors of the Federal Reserve System, Commodity Futures Trading Commission, CFPB, Federal Deposit Insurance Corporation (FDIC), FTC, National Credit Union Administration, Office of the Comptroller of the Currency, and SEC] should assure financial institutions that complying with State mandatory reporting requirements, and reporting suspected elder abuse and fraud in states that do not have mandatory reporting requirements, does not violate the customer's privacy rights under Gramm-Leach-Bliley Act.

In addition, the Executive Office of the President should convene State governors to identify the challenges and share successful strategies that ensure that SAR with information about suspected elder abuse or fraud are transferred to local adult protective services and law-enforcement authorities to protect seniors.

Other ways the Federal Government can protect older Americans is by facilitating and promoting the creation of industry standards for the collection and aggregation of data; requiring financial institutions to adopt commercially reasonable best practices for the use of technologies that detect potential fraud, abuse, or changes in financial capacity; and making rules that will cause financial institutions that offer online banking to create a means for seniors to give monitoring power to a trusted party without enabling that party to initiate transactions, change the senior's profile information, or otherwise engage in fraud or abuse. The SEC should assure financial institutions that holding a transaction due to suspected elder abuse or fraud or impaired capacity does not violate regulations for efficient and timely execution of a transaction, and the FDIC should require financial institutions to routinely offer safe-harbor forms to customers that authorize the institution to share information with a designated family member or other trusted actor if an event of fraud or financial abuse is suspected or discovered.

Recommendation 7: Financial Services

The Federal Government should encourage the banking and financial services sector to offer monitoring services to protect assets from fraud and exploitation.

1. Signatories to the 2013 Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults should accelerate expectations of banks to offer a range of available protective services.
2. The Executive Office of the President should convene State governors to ensure that reports of suspicious activity are reported to relevant adult protective services agencies.

President's Council of Advisors on Science and Technology (PCAST)

www.whitehouse.gov/ostp/pcast