Can Data Sharing Help Financial Institutions Improve the Financial Health of Older Americans?

Larry Santucci*

November 2017

Summary: *This paper explores how increased data sharing among financial institutions could improve the financial outcomes of older adults suffering from cognitive impairment. Among the first signs of cognitive impairment in older adults is a decline in financial capacity, which is also a risk factor for abuse or exploitation. Banks and other financial institutions are at the front lines to monitor and detect changes in financial capacity and susceptibility to fraud and abuse. However, industry experts have found that, in many cases, no mechanism exists for financial service providers to communicate signs of cognitive impairment, abuse, or fraud to family, financial caregivers, or other financial institutions. Creating a regulatory environment whereby financial institutions can more easily share data among themselves could be an important component of a more comprehensive strategy to bridge the communication gap and reduce the frequency and severity of financial losses for older adults.*

Keywords: elder fraud, financial exploitation, Gramm-Leach-Bliley Act, data privacy

JEL Classification Codes: D18, G18, J14

* Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: larry.santucci@phil.frb.org. The author thanks Jason Karlawish and Chantel Gerardo for reviewing and editing several drafts of the paper. Thanks also to Kenneth Benton, Lisa Bleier, Sharon Graham, Jilenne Gunther, Naomi Karp, Surya Kolluri, Suzanne Schmitt, Joseph Snyder, and Jack Terruso for their valuable comments and suggestions. This paper is available free of charge at www.philadelphiafed.org/consumer-finance-institute/payment-cards-center/publications.

1. Introduction

Our cognitive abilities decline as we age, as does our ability to independently manage our finances.[1] As a result, tasks such as the ability to pay bills or read a bank statement become increasingly difficult. A heightened sense of optimism and an inability to assess risk accurately make us more likely to exercise poor financial judgment. These and other challenges to our financial capacity — our ability to manage daily household financial affairs and make sound financial judgments — cause us to be more susceptible to the persuasion of bad actors, particularly those within our own families. For this reason, older consumers are often the targets of financial exploitation and fraud at a cost of billions of dollars annually.[2]

Banking mistakes and poor investment decisions tend to be among the earliest signs of declining financial capacity. Since older adults tend to conduct financial transactions in person, frontline employees such as tellers, branch managers, and financial advisors may be the first to detect changes in an older customer's behavior or cognitive ability.[3] Being able to identify such a change puts the financial institution (FI) in the unique position of knowing something about the client's financial vulnerability that the client's other FIs may not know.[4] While the FI may be able to prevent losses from occurring in accounts held with it, FIs generally are not permitted to share that information with each other.[5] Thus, information valuable to the detection and prevention of future financial losses goes underutilized.

---

[1] Anek Belbase and Geoffrey T. Sanzenbacher, "Cognitive Aging and the Capacity to Manage Money," Center for Retirement Research *Brief*, 17-1, January 2017, available at http://crr.bc.edu/wp-content/uploads/2017/01/IB_17-1.pdf.

[2] "The MetLife Study of Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation Against America's Elders," MetLife, June 2011, available at https://tinyurl.com/chto75f. The study estimated that older victims lose at least $2.9 billion annually from financial abuse.

[3] The Board of Governors of the Federal Reserve System, "Insights into the Financial Experiences of Older Adults: A Forum Briefing Paper," July 2013, available at https://www.federalreserve.gov/econresdata/older-adults-survey/July-2013-Use-of-Financial-Products-and-Services-by-Older-Adults.htm.

[4] For the remainder of the paper, we use the term *financial institution* to refer to brokers, broker-dealers, banks, credit unions, and thrifts.

[5] One exception to this is the USA PATRIOT Act of 2001, discussed further in Section 3.

This paper examines how an industrywide data sharing system could mitigate the loss of valuable information on consumer financial capacity and susceptibility to fraud and exploitation. Section 2 explains how shifting demographics will create an increasingly urgent need to address issues of aging and financial vulnerability. Section 3 presents two common examples of situations faced by older adults. In the first, a woman is the victim of financial fraud. In the second, a man experiencing impaired cognitive function has difficulty managing household finances. Section 4 discusses how a data sharing system could have benefited the older person in each example and explains how consumer privacy and data confidentiality laws affect FIs' ability to share information in elder financial abuse or exploitation cases. Section 5 discusses some of the potential disadvantages of a data sharing system, and Section 6 concludes.

2. A Growing Concern

In the coming years, the number of Americans in need of assistance with banking and investment activities as well as protection from financial fraud and abuse is projected to grow.[6] In 2015 there were 44.6 million Americans aged 65 and older.[7] The Centers for Disease Control and Prevention estimates that, by 2030, that number will increase to 71 million, comprising roughly 20 percent of the population.[8] This estimated growth is due to a combination of factors, including improved health and working conditions, as well as the demographic "bubble" produced by the baby boomers (persons born between

[6] Jennifer M. Ortman, Victoria A. Velkoff, and Howard Hogan, "An Aging Nation: The Older Population in the United States," U.S. Census Bureau *Current Population Reports*, May 2014, available at https://www.census.gov/prod/2014pubs/p25-1140.pdf.

[7] Source: U.S. Census Bureau, 2011–2015 American Community Survey 5-Year Estimates, available at https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk.

[8] Centers for Disease Control and Prevention and The Merck Company Foundation, "The State of Aging and Health in America," 2007, available at http://www.cdc.gov/Aging/pdf/saha_2007.pdf.

What Is Cognitive Impairment?

Cognitive impairment in older adults describes a condition in which a person's everyday life is affected by memory loss or problems with the abilities to concentrate, learn new things, or make sound decisions. The degree of impairment can range from mild to severe.

Mild cognitive impairment occurs when a person experiences changes in cognitive function, although the person is still able to live independently.

The term *dementia* describes a more severe decline in cognitive function in which patients often require assistance with daily activities. In 60 to 80 percent of the cases, dementia is caused by *Alzheimer's disease*. Most of the remaining cases are from *vascular dementia*, which can occur after a person experiences a stroke.

1946 and 1964). With the exception of an increased prevalence of obesity, Americans are much healthier today than they were 40 years ago. According to the National Center for Health Statistics (NCHS), throughout 1975 to 2015, heart disease and cancer were the first and second leading causes of death in America. However, during that time, the age-adjusted heart disease death rate decreased by 61 percent and the age-adjusted cancer death rate decreased by 21 percent. With improved health comes increased longevity. The NCHS also notes that, between 1975 and 2015, the life expectancy at birth for all Americans increased from 72.6 to 78.8 years, with the life expectancy for women reaching 81.2 years.[9]

Despite — or perhaps as a result of — improvements in overall health and increased longevity, neurodegenerative diseases have become more prevalent. Mild cognitive impairment (MCI) and various forms of dementia are increasingly common with aging, especially after age 70.[10] Research conducted using the University of Michigan's *Health and Retirement Study* for the period 1994–2014 indicates that 12 percent of the population aged 70–74 was diagnosed with MCI or dementia. In people aged 85 and older, the prevalence of dementia or MCI is 64 percent. Women are more likely to develop dementia than men. Women will also comprise the majority of persons living to age 85 and beyond, many of whom

[9] National Center for Health Statistics, "Health, United States, 2016: With Chartbook on Long-term Trends in Health," Hyattsville, MD, 2017.

[10] Please refer to the box on this page for more information on cognitive impairment.

were less likely than their spouse to manage household finances.[11] Such population characteristics will exacerbate the need for innovative solutions and age-friendly banking products in the 85 and older demographic segment.

3. Two Examples of Cognitive Impairment and Financial Loss

The following two vignettes are based on anecdotes that industry experts shared with the author.[12] The first vignette presents a common elder fraud scheme known as the "grandparent scam." According to the Federal Trade Commission, imposter identity scams surpassed identity theft as the second most common category of consumer complaints in 2016.[13] In the second vignette, an older man is showing signs of cognitive impairment but cannot admit it to himself or his family.

a. Mrs. Wallace

Late one night, Mrs. Wallace was awoken by a phone call from someone purporting to be her grandson. The person told Mrs. Wallace, a 77-year-old widow, that he'd been involved in some trouble and needed $2,000 to pay for a lawyer. The person asked Mrs. Wallace to wire the money to the law firm's bank account. The next morning, Mrs. Wallace went to the bank and asked the teller to initiate a wire transfer. Although suspicious of the transaction, the teller went ahead with the transfer. Bank policy did not require a manager to be notified or any reports to be filed, and no notices needed to be posted to Mrs. Wallace's account.

---

[11] See Annamaria Lusardi and Olivia S. Mitchell, "Baby Boomer Retirement Security: The Roles of Planning, Financial Literacy, and Housing Wealth," *Journal of Monetary Economics*, January 2007, 54 (1), pp. 205–224, an earlier version of which is available at www.nber.org/papers/w12585.pdf. See also Joanne W. Hsu, "Aging and Strategic Learning: The Impact of Spousal Incentives on Financial Literacy," FEDS Working Paper 2011-53, available at http://dx.doi.org/10.2139/ssrn.1969411.

[12] Pseudonyms are used in place of real names.

[13] See the Consumer Sentinel Network Data Book for January–December 2016, available at https://tinyurl.com/juk8uvd.

A few days later, the grandson called again. This time, he needed $5,000 to pay his court fine, or he would have to spend three months in jail. Mrs. Wallace told the person that she did not have that much money in her savings account. The person suggested she use funds from one of her investment accounts. She complied and called her financial advisor to request a transfer.

At the brokerage firm, the financial advisor politely asked Mrs. Wallace about the transfer. The advisor became suspicious after learning the money was for a grandson who was in trouble. The firm's policy required that the advisor escalate the incident to her manager before allowing it to be authorized. The manager called Mrs. Wallace and politely explained that other people had been fooled by criminals posing as relatives in trouble, and asked Mrs. Wallace if she was certain the person on the phone had been her grandson. Mrs. Wallace insisted it was, and that the transfer be processed so that her grandson could get out of jail. The manager and financial advisor went back and examined Mrs. Wallace's account records to see if an emergency contact was listed, but there was none. They also reviewed Mrs. Wallace's account history. Before this incident, there had never been a red flag that suggested Mrs. Wallace was having problems managing her money. The manager authorized the transfer.

A month later, Mrs. Wallace received a phone call from a woman claiming to be an attorney at a local law firm. The person explained that Mrs. Wallace's grandson had never been in trouble and that she had been scammed. Fortunately, the person said, for $800, her firm could open a case for her and recover the $7,000. Mrs. Wallace went back to her bank, this time to another teller, and wired the money to the person's bank account.

b. Mr. Davis

Mr. Davis is a retired dentist. For more than 40 years, he has been managing the household finances, seeing three children through college and borrowing to finance his private practice. His weekly responsibilities include paying bills and reconciling bank and credit card statements. He regularly uses online banking portals and pays many bills online. His retirement savings is spread between three

institutions: a large regional credit union, a self-service investment management company, and a national bank/brokerage firm.

Recently, Mr. Davis received a notice in the mail saying that he had been assessed a $25 late fee for not paying his credit card bill. Over the next few days, he received similar notices from his telephone and cable providers and a bill from a medical imaging center with $5 added for late payment.

Certain that it was a mistake, Mr. Davis called his credit union and asked a customer service representative why his payments had not been processed. The representative had Mr. Davis log into the credit union's online portal and directed him to the transaction history, where there was no evidence that the bills were paid during the previous month. Mr. Davis was bewildered. On his desk, where unpaid bills usually sit, he was surprised to find none of the previous month's bills. Had he thrown them away without paying? Embarrassed, he paid the past due amounts immediately and decided to say nothing to his wife, hoping that it would not happen again.

Over the next several months, Mr. Davis took extra care to pay his bills on time, sometimes using double and triple reminders. Any bill that could be paid automatically is now set up in the online banking system. However, during that time, he experienced several episodes when he forgot where he was driving and what he needed to do. Rather than call his wife to remind him, he returned home empty handed.

Is It Financial Fraud or Financial Exploitation?

The distinction between elder fraud and financial exploitation has important consequences for the interpretation of laws regulating data privacy and confidentiality.

The U.S. Department of Justice defines *elder fraud* as an act targeting older adults in which attempts are made to deceive with promises of goods, services, or financial benefits that do not exist, were never intended to be provided, or were misrepresented. Financial scams targeted toward older adults are a common form of elder fraud.

The National Center on Elder Abuse defines *elder financial exploitation* as the illegal or improper use of an elder's funds, property, or assets. Elder financial exploitation is generally considered a type of elder abuse. Examples include:

- Cashing an elderly person's checks without authorization or permission
- Forging an older person's signature
- Misusing or stealing an older person's money or possessions
- Coercing or deceiving an older person into signing any document
- The improper use of conservatorship, guardianship, or power of attorney

4. Confidentiality Laws and Information Sharing

Often, the first poor financial decision made by someone suffering from cognitive impairment is not the last. Poor decisions, fraud susceptibility, and exploitation can spread like a contagion throughout the person's financial portfolio. As demonstrated in the example of Mrs. Wallace, once someone falls victim to a financial scam, the person tends to receive additional scam offers, some of which purport to have the ability to recover funds lost from the previous scam.[14] In other instances, a fraudster may initiate a Ponzi-style series of payments from one older person to another, ultimately ending in a payment to the

[14] These are known as *refund and recovery* scams. See https://tinyurl.com/ybqpnu4g.

fraudster.[15] In both cases, a data sharing system could help stem the contagion by providing a means for FIs to communicate warnings about common clients to each other.

If Mrs. Wallace's bank teller been able to notify her financial advisor of the suspicious account activity, the advisor might have chosen to escalate the incident and request that a temporary hold be placed on the transaction.[16] Likewise, if the advisor then notified the bank of a second suspicious transaction, the bank could have placed a note in Mrs. Wallace's account alerting tellers to take a closer look at future transactions and to route suspicious ones immediately to the compliance officer at corporate headquarters.

With the help of his credit union, Mr. Davis was able to realize his mistake and use online banking tools to safeguard against missed payments in the future. However, if his condition progresses, Mr. Davis could become susceptible to making poor investment decisions, become the victim of a financial scam, or be exploited by a trusted family member or investment advisor. A data sharing system would enable Mr. Davis's credit union to notify his investment management company and bank/brokerage firm of the need to closely monitor his accounts for suspicious activity.

In recent years, financial industry regulators have encouraged certain kinds of information sharing. Legislation passed in 2001 permitted FIs to share personal consumer information directly with each other but only in matters of suspected money laundering or suspicion of terrorist financing.[17] In

---

[15] The source of this example is F. Scott Dueser, Chairman, President and CEO, First Financial Bankshares, Inc. In a typical Ponzi scheme, existing investors are paid "returns" from funds contributed by new investors; see https://www.sec.gov/fast-answers/answersponzihtm.html.

[16] Many states have so-called report and hold laws designed to protect older people from financial exploitation. Whether the law covers elder fraud may depend on the particular statute. Report and hold laws generally authorize disclosure to Adult Protective Services as well as a trusted contact, provided the contact is not the person suspected of committing the crime. The laws also permit delays in disbursing funds. A version of the North American Securities Administrators Association (NASAA) Model Act has been passed by 13 states. The NASAA Model Act is available at https://tinyurl.com/ya7a8ovd. Beginning on February 5, 2018, FINRA Rule 2165 will allow member organizations to place a temporary hold on disbursement of funds or securities under certain circumstances. See https://tinyurl.com/y8k6qkcb.

[17] Section 314(b) of the USA PATRIOT Act (31 CFR 1010.540)

2013, a group of eight banking regulators issued guidance clarifying that FIs may share the consumer's personal information with federal, state, and local investigators when elder financial fraud or exploitation is suspected and still be compliant with financial consumer privacy laws.[18] That same year a federal financial crimes reporting system linking FIs with financial crimes investigators was enhanced to include a specific check box for elder financial exploitation.[19] Unfortunately, these changes have neither encouraged nor facilitated information sharing *between* FIs for the purpose of preventing elder financial crimes.

The next section discusses financial consumer privacy laws and exceptions to those laws that permit FIs to share personal consumer information with certain nonaffiliated organizations, noting that guidance issued jointly by financial industry regulators presented a restrictive interpretation of the exceptions that effectively prohibited information sharing between FIs.[20] We then examine an existing system that is already being used to share information between FIs for other purposes.

a. Confidentiality of Personal Information

At the federal level, data privacy and confidentiality in the financial services industry are governed by several statutes, including the Federal Trade Commission Act, the Right to Financial Privacy Act, the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA).[21] In particular, the GLBA restricts FIs' ability to share nonpublic personal information (NPI) with nonaffiliated third

---

[18] See Fed. Reserve, CFTC, CFPB, FDIC, FTC, NCUA, OCC, and SEC, Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults (September 23, 2013), available at https://goo.gl/ZNAajK.

[19] FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Instructions, Version 1.2 (October 2012), p. 98, available at https://goo.gl/zAin7J.

[20] See footnote 16.

[21] Federal Trade Commission Act (15 U.S.C. §41 et seq.); Right to Financial Privacy Act (12 U.S.C. §3401 et seq.); Fair Credit Reporting Act (15 U.S.C. §1681 et seq.); Gramm-Leach-Bliley Act (GLBA; 15 U.S.C. §6801 et seq.); individual states also have their own confidentiality laws, as many enacted a version of the RFPA. See Jeffrey Heuer, "A Brief History of Bank Privacy," Lexology.com, blog entry, September 8, 2016, available at www.lexology.com/library/detail.aspx?g=6150ba14-01b0-4c6b-bc31-51b7308b8ea0.

parties.[22] Its restrictions apply to a wide range of FIs, including banks, securities brokers and dealers, insurance companies, mortgage bankers, and finance companies, as well as third-party companies that handle financial NPI. Except in certain cases, the GLBA prohibits FIs from disclosing NPI to nonaffiliated third parties without first notifying the consumer of how the information will be used as well as providing an opportunity to opt out. If, after being notified of the opportunity to opt out the consumer does not do so, the FI is permitted to disclose the consumer's NPI to any nonaffiliated third party. On the other hand, for consumers exercising their right to opt out, an FI may only disclose NPI under certain circumstances. Section 502(e) of the GLBA lists several exceptions to the notice and consent requirements. In particular, FIs may disclose NPI to a nonaffiliated third party without notice or consent in certain circumstances, including:

- to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
- for required institutional risk control, or for resolving customer disputes or inquiries;
- to law enforcement agencies, to the extent specifically permitted or required under applicable law;
- to comply with federal, state, or local laws, rules, and other applicable legal requirements;
- to comply with a properly authorized civil, criminal, or regulatory investigation, subpoena, or summons by federal, state, or local authorities, or to respond to judicial process or governmental regulatory authorities having jurisdiction for examination, compliance or other purposes.

The first exception permits FIs to disclose NPI to nonaffiliated third parties when they believe elder fraud — including a financial scam — has occurred or is likely to occur. In addition, to the extent that financial fraud risk is considered a form of institutional risk by the relevant regulatory agency(ies),

[22] According to the GLBA, the term *nonaffiliated third party* is any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the FI but does not include a joint employee of such institution.

What Is Adult Protective Services?

According to the National Adult Protective Services Association, few states offered protective services to people over the age of 18 before 1975. However, once states were permitted to use federal funds for such programs, they began mandating that their social service agencies provide both casework and delivery of protective services to adults. By 1978, almost 20 states had enacted legislation, and by 1985, 46 states had an office responsible for the delivery of Adult Protective Services (APS).

While each state created its own laws and regulations, most followed a similar model. Thus, APS programs typically provide elder abuse victims with both social and health services that are designed to enable older adults to continue living at home and to protect them from abuse. To do so, the agencies receive reports, conduct investigations, evaluate client risk and capacity to agree to services, develop and implement case plans, and arrange for the client to receive a variety of services and benefits.

See www.napsa-now.org/about-napsa/history/history-of-adult-protective-services/.

second exception may permit disclosure for the purpose of controlling institutional exposure to such risks.

The final three exceptions permit FIs to report NPI to law enforcement agencies and to comply with federal, state, and local laws. Since most states require employees of FIs to report suspected abuse, neglect or exploitation of adults to adult protective services (APS), these exceptions are necessary to ensure that FIs complying with state APS laws do not conflict with federal confidentiality restrictions.[23] Since APS agencies are authorized under state and tribal law to receive and investigate reports of elder abuse, the GLBA permits FIs to disclose NPI with APS agencies functioning as a social service under the final exception.

Although, as described previously, the GLBA exceptions permit FIs to share information with nonaffiliated third parties when they detect evidence of elder fraud or financial exploitation, many FIs have historically tended to err on the side of caution when interpreting the GLBA, resulting in the underreporting of suspected exploitation to APS and a reluctance to notify family members of the affected

[23] See www.napsa-now.org/get-help/how-aps-helps/ and the Consumer Financial Protection Bureau, "Recommendations and Report for Financial Institutions on Preventing and Responding to Elder Financial Exploitation," March 2016, available at https://tinyurl.com/ycg9rbbh.

consumer.[24] The 2013 joint guidance discussed previously was an attempt to clarify the applicability of the GLBA privacy requirements. However, it does not appear to have provided sufficient clarity or flexibility, nor does it constitute a rewriting of the GLBA. The guidance states that the GLBA's 502(e) exceptions permit reporting elder financial exploitation to local, state or federal agencies but does not extend protections to sharing with other nonaffiliated third parties.[25]

b. Secure Information Sharing System

While currently prohibited, legislative changes could allow FIs to communicate with each other in matters of fraud or exploitation through the U.S. Department of Treasury's web-based Secure Information Sharing System (SISS), administered by the Financial Crimes Enforcement Network (FinCEN). SISS was created as a result of Title III of the USA PATRIOT Act of 2001 (PATRIOT Act), which directed the Department of Treasury to establish a secure electronic network for communication between financial institutions and law enforcement agencies. FIs participating in SISS are provided a safe harbor from liability for disclosing NPI to another FI in order to better identify and report potential money laundering or terrorist activities.[26] Participation is voluntary and requires annual registration.[27]

Along with maintaining an information sharing system, FinCEN also collects data on elder financial exploitation. Among the better-known provisions of the Bank Secrecy Act (BSA; 31 U.S.C. §5311 et seq.) is the Suspicious Activity Report (SAR) requirement. While it is primarily used to prevent money laundering, tax evasion, and — since 2001 — the financing of terrorist activities, the SAR

---

[24] Sandra L. Hughes, "Legal Issues Related to Bank Reporting of Suspected Elder Financial Abuse," American Bar Association Commission on Law and Aging, 2003, available at https://tinyurl.com/ycfjrnfo.

[25] See footnote 16. Specifically, the guidance states that the GLBA's 502(e) exceptions permit the reporting of "incidents that result in taking an older adult's funds without actual consent" and "obtaining an older person's consent to sign over assets through misrepresentation of the intent of the transaction."

[26] See https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf. The particular safe harbor provision can be found in Section 314(b) of the PATRIOT Act.

[27] Banks, bank holding companies, and bank subsidiaries must comply with the BSA, as do broker-dealers regulated by the Securities and Exchange Commission. The latter requirement is attributable to Rule 17a-8 (17 CFR 240.17a-8) promulgated under the Securities and Exchange Act.

requirement has become an important component in the reporting and investigation of elder financial abuse. In 2011, FinCEN issued an alert that encouraged FIs to file a SAR when they suspected that elder financial exploitation had occurred.[28] Then, in 2013, FinCEN created an electronic filing form that included a specific check box for FIs to indicate suspicion of elder financial exploitation.[29] If the electronic SAR forms were integrated into the SISS data sharing system, the two capabilities could provide a low-cost, federally administered framework for interinstitutional information sharing.

5. Potential Disadvantages of Data Sharing

The benefits of allowing FIs to share NPI in order to cease or prevent elder fraud or financial exploitation seem clear. Information sharing enables FIs to act as a single, unified consumer protection tool, independently learning about their customers' financial behavior, but acting jointly to protect the consumer's assets when they are being exploited. There are, however, a number of reasons why allowing information sharing between FIs could have costly consequences for both the consumer and the institutions involved. For one, data residing in multiple locations, particularly external locations, creates additional targets and access points for hackers to steal customer data. FIs participating in a multi-institution internal investigation can also risk oversharing- unintentionally sharing more customer information than what is required for the investigation. In either case an FI risks losing control of its data and exposing itself to liability.[30]

Data security and oversharing are not the only risks to information sharing. FIs receiving data about one of their customers from another institution must also judge whether the information constitutes a credible and material threat to the customer or the organization and, if so, what action to take as a result

---

[28] See https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2011-a003.

[29] See https://tinyurl.com/yavkrdr7. Cases of suspected fraud are presumably described as such in the Suspicious Activity Information section of the SAR form.

[30] FIs are responsible for ensuring that third-party service providers comply with data security protocols set forth in Section 501(b) of the GLBA. Thus, depending on the structure of the data sharing system, FIs might also be responsible for ensuring any third parties involved in the ongoing operation or hosting of the system also comply with the GLBA.

of the information. Not taking action when an alert has been posted opens up the possibility for a preventable event to occur, while overreacting to a dubious alert risks offending the customer and possibly losing their business.

As an example, suppose Bank A notifies other FIs in the information sharing system of a case of suspected financial exploitation by a person listed as a trusted contact and power of attorney on a savings account. If the particular customer is also a client of Bank B's, then, before taking any action on the client's behalf, Bank B might consider whether information received from Bank A has been credible and reliable in the past. If Bank A has a history of submitting notifications that have failed to identify an elderly person who is truly at risk, Bank B might put little weight on subsequent notifications from Bank A.

Bank B might also look into its own records to determine whether it provides additional insight into the customer's current financial situation, the relationship between the customer and the trusted contact, or the destination of funds being transferred from the savings account at Bank A. Suppose that, as a result of past experience with Bank A or proprietary client information, Bank B decides to continue to monitor the customer's accounts, but take no further action. If an exploitative transaction were then to affect the customer's accounts at Bank B, the bank might have to defend its decision to not take immediate action to an investigator, regulator, or judge.

At the other extreme, suppose that Bank B determines that the customer's assets are in jeopardy and places a temporary hold on a suspicious withdrawal, only to find that the transaction was not exploitative and in fact was necessary to cover an unanticipated expense. As a result of the bank's actions, the customer may have bounced a check or become delinquent on a credit account and been assessed a late fee. This situation could result in a complaint being filed with a regulator and a loss of the customer's business.

Thus, having access to another FI's information may not necessarily result in better outcomes for either the customer or the other FIs involved. FIs receiving outside information will have to learn how to process the information along many dimensions, including the perceived quality of the reporting

institution's information, the perceived quality of the signal, the type of signal received, and the relationship with the customer. A mistake or miscalculation along any of those dimensions could have more detrimental repercussions for the customer and institution than if it hadn't had the information at all. Encouraging FIs to exercise their own judgment when it comes to outside information may require the creation of safe harbor provisions preventing consumers from bringing suits against an FI that does not act on information received from another FI.

6. Conclusion

As the U.S. population ages into retirement, matters of financial capacity will become increasingly important for retirees, their family members and caretakers, and the FIs upon which they rely for banking, payment, and investment services. The stakes are high; affected seniors will inevitably experience a standard of living that decreases with the amount of money lost. In extreme cases, some will outlive their savings or be unable to afford critical medical attention or long-term care.

Section 3 relayed the fictionalized stories of two older adults. In both examples, the person could have benefited from their bank, credit union, or broker sharing information with the other institutions with which the person did business. A data sharing system could have helped the FIs share information gleaned through their individual client interaction to protect older clients from financial losses in accounts held at other FIs. Unfortunately, with the exception of the limited sharing permitted under the PATRIOT Act's voluntary model, FIs are not provided safe harbor from the information sharing restrictions imposed by the GLBA's privacy provisions and thus cannot safely share information with each other in matters of elder financial abuse, exploitation, or cognitive decline. FIs also lack clear and consistent assurances from regulatory agencies that good faith information sharing will not result in additional liability or regulatory enforcement action.

With both an electronic reporting system for suspicious activities and a secure data sharing system, lawmakers and regulators should consider leveraging FinCEN's existing resources to develop a dedicated interbank data sharing network for elder financial crimes. Housing the system within FinCEN

would not only be cost-effective but would also resolve the issue of database administration. While such a data sharing system would not be without its disadvantages and would require a good deal of planning, strategy, and judgment on the part of all participating FIs, there appears to be clear value in facilitating some kind of interinstitutional communication in matters of elder financial fraud and exploitation.

FEDERAL RESERVE BANK OF PHILADELPHIA

Payment Cards Center Discussion Paper Series

http://www.philadelphiafed.org/PCC