



True Link

The True Link
Report on
Elder Financial
Abuse 2015

January 2015

About True Link Financial

True Link Financial is a San Francisco, California-based financial services firm that helps seniors and their families protect themselves from fraud, exploitation, and financial abuse. The company offers tools to detect suspicious activity and block unwanted transactions, preserving seniors' independence and keeping their money safe. True Link's data science team is dedicated to building world-class tools that prevent elder financial abuse and sharing its research to aid others also working toward that vision.

The survey research underlying this report was produced as a collaboration between the True Link data science team and Laurie Orlov. Orlov spent nine years as a leading industry analyst at Forrester Research before founding an independent research and analysis firm focused on aging. She has produced numerous research studies related to aging on behalf of clients such as Philips and AARP.

For more information about True Link Financial, please visit:
www.truelinkfinancial.com.



True Link

© 2015 True Link Financial

Table of Contents

Executive Summary	1
Research Goals	4
Reconcile discrepancies among previous studies	4
Align research with accepted definitions of elder financial abuse	5
Gain a deeper understanding of sources of vulnerability	6
Methodology	7
Findings	11
Magnitude of elder financial abuse	11
Criminal Fraud	11
Caregiver Abuse	13
Financial Exploitation	15
The financial exploitation progression	17
Non-financial effects of financial abuse	18
Risk factors	19
Reporting and underreporting	23
Conclusion	25
Appendix A: Common Examples	26
Appendix B: Significant Risk Factors	35
Endnotes	36



Executive Summary

Prior to this report, the most frequently cited estimate of the amount of money lost to elder financial abuse was \$2.9 billion. In the fraud research community, we have long suspected that this was an underestimate. In fact, it is a dramatic underestimate: our research reveals that seniors lose \$36.48 billion each year to elder financial abuse. This is more than twelve times what was previously reported. Approximately 36.9% of seniors are affected by financial abuse in any five-year period.

Breakdown of the problem

- **Financial exploitation:** \$16.99 billion is lost annually to financial exploitation, defined as when misleading or confusing language is used—often combined with social pressure and tactics that take advantage of cognitive decline and memory loss—to obtain a senior’s consent to take his or her money.
- **Criminal fraud:** \$12.76 billion is lost annually to explicitly illegal activity, such as the grandparent scam, the Nigerian prince scam, or identity theft.
- **Caregiver abuse:** \$6.67 billion is lost annually to deceit or theft enabled by a trusting relationship—typically a family member but sometimes a paid helper, friend, lawyer, accountant, or financial manager.

Sources of risk

- People often assume that those perceived as most vulnerable—widows, the very old, people with severe memory loss—are at greatest risk. In fact, risk equals vulnerability plus exposure. Seniors who are young, urban, and college-educated lose more money than those who are not.
- Some sources of exposure were surprising. Seniors described as extremely friendly lose four times as much to elder financial abuse,

perhaps because they are approachable and may give strangers the benefit of the doubt. Financially sophisticated seniors lose more to fraud, likely because they are comfortable moving larger amounts of money around. Thrifty seniors lose five times as much to fraud, perhaps because they are enticed by bargains.

The exploitation progression

- Small losses are evidence of an underlying vulnerability. What seems like an isolated incident is often the first step in a financial exploitation progression. A senior who lost as little as \$20 in a year to exploitation could be expected to lose \$2,000 a year to other types of fraud.
- A person who receives just one telemarketing phone call per day is likely to experience three times as much financial loss as someone who receives no or only occasional telemarketing calls.

Non-financial effects

- Financial abuse frequently results in reduced emotional and physical health for seniors. We estimate that 954,000 seniors are currently skipping meals as a result of financial abuse.

Research methodology

The primary source of data analyzed in this report is the 2015 True Link Senior Vulnerability Survey, a survey of family caregivers for older Americans that includes 2,335 cumulative years of data on incidents of financial abuse. The design of this survey was guided by the recommendations of an expert panel of fraud researchers convened by the Financial Fraud Research Center at the Stanford Center on Longevity.

Summary findings

Category	Annual cost to seniors	Avg. five year loss	Defining feature	Examples
Exploitation	\$16.99 billion	\$2,617	Operating openly claiming consent of the victim	<ul style="list-style-type: none"> • Hidden shipping and handling or subscriptions • Work-from-home schemes • Quack weight loss or dietary products • Excessive gifts • Misleading financial advice¹
Criminal fraud	\$12.76 billion	\$13,107	Anonymous illegal activity	
<i>Con artists</i>	\$9.85 billion	\$13,225	Attempt to get you to give them money	<ul style="list-style-type: none"> • Grandparent scam • Nigerian prince emails • Fake lottery winnings or government grants • Sweetheart scam
<i>Identity theft</i>	\$2.91 billion	\$7,633	Opening or using accounts without authorization	<ul style="list-style-type: none"> • Opening new credit cards, bank accounts, or payday loans • Car title or home equity loans on your property • Using card data gained by phishing, in data breach, or from the mail
Caregiver abuse	\$6.67 billion	\$26,879	Abuse of trusting relationship	<ul style="list-style-type: none"> • Theft by family members or caregivers • Rewritten wills or powers of attorney • Borrowing money hoping senior will forget • Sometimes combined with physical abuse or neglect
Total losses	\$36.48 billion²	\$11,583		

Research Goals

Elder financial abuse³ is no longer the “silent epidemic” it used to be. This once-ignored issue is beginning to get the attention it deserves, everywhere from the Senate Floor to the Nightly News. Yet we still know so little about it. How many people are affected? How much money is lost? Who is most likely to be a victim? To be a perpetrator? Why?

Although the answers to those questions are the subject of spirited debate in the elder abuse prevention community, we can all agree that to begin to solve this problem we need to understand it better. This report and the data herein represent our contribution to that endeavor. We hope that our report aids all of us in protecting ourselves and our families, and that it informs and inspires all of those working to protect our society’s most vulnerable, whether through policy, the press, or practice.

Reconcile discrepancies among previous studies

Our first goal in publishing this study is to reconcile discrepancies in a set of known facts about elder financial abuse. On the one hand, across studies by the Federal Trade Commission and others, it is reported that approximately fifteen percent of Americans fall victim to fraud every year.⁴ Older adults have been shown to be more vulnerable than the general population to almost every type of financial abuse.⁵ It is also known that changes in the brain that occur during the aging process create extra sources of vulnerability.⁶

On the other hand, the most frequently cited estimate of the cost of elder financial abuse is surprisingly low—\$2.9 billion, from a 2011 study by the MetLife Institute.⁷ To develop that estimate, the MetLife study added up the financial losses reported in three months of published news stories, despite research consistently finding that more than 90% of financial exploitation of seniors goes unreported.⁸ While the MetLife study was based on an estimate of approximately two thousand instances of fraud every year, other research indicates that closer to six million seniors fall victim to fraud every year.⁹ Clearly, we have not been getting the complete picture.

Furthermore, when you look closely at any specific category of fraud, the numbers start to balloon. In the 1990s, a Congressional panel found that telemarketing fraud alone cost as much as \$15 billion a year, primarily targeting seniors.¹⁰ Likewise, the Investor Protection Trust found that one in five seniors had been affected by a financial swindle.¹¹ Individual states alone estimate that their residents face a considerable share of the abuse that MetLife reports at a national level.¹² Our own experience at True Link with our customers and their families made it clear to us that the numbers must be much greater than previously reported.

Align research with accepted definitions of elder financial abuse

Second, we wanted to capture mass-market financial exploitation. So often, the ways older adults are defrauded appear to be legal because of a disclaimer or fine print. Maybe the salesperson didn't actually lie, but just said something confusing that led to an unexpected, unwanted, or unnecessary charge. It is clear that deceptive practices like these should be included in any definition of elder financial abuse.

The law varies from jurisdiction to jurisdiction, but across the board it is illegal to deceptively profit from the infirmity of an elderly person¹³—and the relationship between aging and vulnerability is now an established medical fact. We also know that the public agrees with this broad legal definition. In the 2014 True Link Financial Abuse Perceptions Survey, we surveyed over seven thousand American adults about their perspectives on what constitutes elder financial abuse. Our results conclusively showed that, whether you technically lied or not, if a senior misunderstood something and gave you money as a result, it is exploitation and abuse in the public's view.

In summary, the law and the public both define deceptive marketing and sales tactics as abuse, yet these are so rarely reported in the press or pursued by law enforcement that no one is looking into this as a systematic problem. Adding

The law and the public both define deceptive marketing and sales tactics as abuse.

deceptive marketing to our understanding of elder financial abuse is critically important to ensuring that the public is prepared to fight back against the “crime of the 21st century.”¹⁴

Consistent with both public opinion and the law, for the purposes of this study, we defined elder financial abuse as any time someone took financial advantage of an older adult in a way that would not have been possible when the senior was younger. Previous research has demonstrated that many individuals who report losing money in specific incidents of fraud do not label their experience as “fraud.”¹⁵ Instead of asking people if they were impacted by financial abuse, we asked multiple questions about whether a very specific set of occurrences had happened to them.

Gain a deeper understanding of sources of vulnerability

Third, we sought to identify specific factors that affect vulnerability. Previous studies have often failed to point to such factors.¹⁶ Key studies even disagree about whether older adults are more vulnerable to financial abuse than middle-aged and young adults.¹⁷ This appears to be because factors—often countervailing ones—point in different directions. For example, the AARP found that lottery fraud victims were more likely to be women over 70 living alone, with lower education, lower income, and less financial literacy, while victims of investment fraud were more likely to be men between the ages of 55 and 62 who were married, with higher incomes and greater financial literacy.¹⁸ We sought to identify specific factors that may indicate increased risk, which is something we’ve heard is critical time and time again from those working to prevent elder financial abuse.

Methodology

In the course of operating its core fraud protection business for seniors, True Link employs a data science and research team that maintains a database of known types of fraud, including how they operate, how prevalent they are, what the warning signs are, and who is likely to be at risk.

The primary source of data presented in this report is the 2015 True Link Senior Vulnerability Survey. This was a survey of Americans aged 50–70 that used the SurveyMonkey Audience panel in October 2014. Among other things, SurveyMonkey is a survey research and polling partner of NBC News. We contacted 2,096 respondents and asked them to describe the financial issues they experienced in caring for an older adult over the last five years. Filtering to the 467 respondents who identified themselves as having “any responsibility for an older adult,” we collected 2,335 cumulative years of data.¹⁹

The survey asked experiential questions—questions like, “Has the person you care for been asked to send money or provide personal information to help someone posing as a relative or other acquaintance?” and “Has this person been asked to spend money on ‘free’ trials that weren’t free or were hard to cancel?” For “yes” answers, data was collected on how many times the fraud was attempted, whether money was lost, and how much was lost over the five-year survey period.

This methodology was influenced most heavily by two sources: the guidance of an expert panel convened by the Financial Fraud Research Center at the Stanford Center on Longevity, and prior research and internal data about the specific nature of this problem from the True Link data science team and True Link’s customers.

Among the conclusions drawn from their panel of experts, Martha Deevy and Michaela Beals of the Financial Fraud Research Center recommended using survey estimates instead of complaint data, and classifying fraud based on experiential questions (“Did X happen to you?”) rather than questions based on self-identification (“Were you the victim of fraud?”).

They also recommended experimenting with proxy respondents for vulnerable populations with diminished capacity. We believe that by adopting these key expert recommendations, we were able to develop a much more accurate estimate than previous studies, like those conducted by MetLife (2011) or Allianz (2014). For an excellent and thorough discussion of the pros and cons of various survey designs, see Martha Deevy and Michaela Beals, “The Scope of the Problem: An Overview of Fraud Prevalence Measurement” (2013) and “The True Impact of Fraud: A Roundtable of Experts” (2014), both from the Financial Fraud Research Center at Stanford University.²⁰

By adopting these key expert recommendations, we were able to develop a much more accurate estimate than previous studies.

The True Link data science team has conducted four other research activities that informed the methodological approach of this analysis. Critically, each of these data sources provided or clarified specific examples of criminal fraud, exploitation, and caregiver abuse in a way that enabled the development of experiential questions. This research is referenced throughout the report, and more detail will be provided in future reports.

- *The 2014 True Link Financial Abuse Perceptions Survey.* We surveyed 7,422 Americans about their perceptions of financial fraud and exploitation targeting seniors. We used a representative sample of American adults drawn from Google Surveys. We presented participants with various scenarios involving an interaction between a senior and an individual or organization engaging in deceptive or predatory practices. The survey asked respondents to characterize the interaction with questions like, “Was this an example of fraud?”; “Was this an example of financial vulnerability?”; “Was this an example of exploitation?”
- *An anonymized sample of 9,008 Visa card transactions from seniors over 65, provided by True Link’s internal processing.*²¹ Of these transactions, 3,541 represented spending by older adults whose family members were closely monitoring their finances.

- *A set of surreptitious interactions with merchants we believed were engaged in abusive, fraudulent, and exploitive behavior.* We spoke with sales representatives from 208 telemarketers, mail-order and TV merchants, and organizations posing as charities in solicitation activities. Typically, we went through an entire sales process, classifying which tactics they used, which products they cross-sold, how many times they charged card numbers they were given, and which additional organizations they permitted to charge the cards.
- *A set of interviews with 67 True Link customers.* We conducted interviews with both older adults and family members about the types of fraud or financial exploitation they have experienced in the past and are currently facing. We found that for these customers, using True Link protects them from an average of \$2,340 per year of unwanted transactions.

To estimate the total amount of elder financial abuse affecting the U.S. population each year, we calculated the mean annual financial loss per person over 65 implied by our sample and multiplied it by the U.S. population over 65.²² Because the demographically representative panel we used to calculate national average losses was selected for having a family member or other adult with some level of responsibility, we looked carefully for robustness against extrapolation bias. In particular, we looked at possible bias introduced by age and gender deviations against national averages. We found that demographic corrections for age and gender did not substantially affect the results. These were within 15% of the raw figures, with the corrected numbers slightly higher than raw, uncorrected figures. Out of conservatism, we reported the lower, uncorrected number rather than the higher, corrected number.

Second, we looked at bias resulting from adverse selection on family member involvement—the plausible hypothesis being that greater family member involvement might be correlated with the unobserved hidden variable of underlying vulnerability. We found that within our panel, level of family member involvement was unrelated to financial losses. For example, people who have a family member who reviews their finances at least once a month suffered greater financial losses than people whose family members only rarely or never review

their finances. It is likely that we introduced underreporting effects by including family members who reported never reviewing seniors' finances, as especially with small-dollar exploitation, they might not be aware of the abuse taking place. However, we could not devise a better way to limit underreporting without introducing bias.

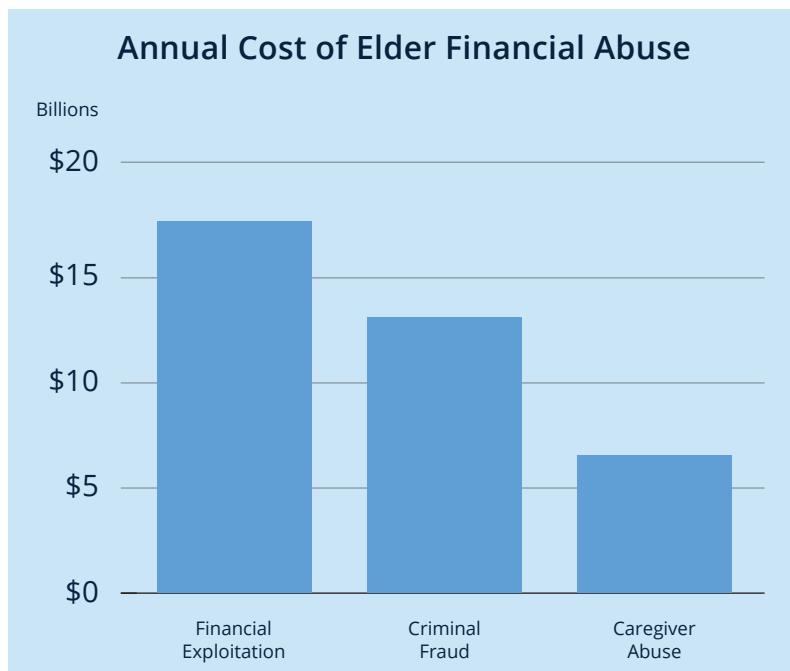
We used linear regression to model the relationship between financial losses and the independent variables (e.g., age, education level, friendliness throughout the course of one's life) and logistic regression to model the likelihood of losses.



Findings

Magnitude of elder financial abuse

We estimate that financial abuse costs American seniors a total of \$36.48 billion per year. We also found that approximately 36.9% of seniors are affected by financial abuse in a given five year period.



Criminal fraud

We divided our assessment of abuse into several categories. ***Criminal fraud*** is defined as any money-taking activity perpetrated by a criminal who is concealing his or her identity to avoid getting caught.²³ The key signal we used to classify an event as fraud was that the perpetrator had clearly embraced the fact that the activity was illegal. Such perpetrators operate anonymously; they make statements in writing that are overt lies; they are often from foreign jurisdictions with low levels of law enforcement. These are not people who assume that if they ended up in a courtroom, they could get off the hook. They are people who are diligently avoiding the courtroom altogether.

We further broke down criminal fraud into two subcategories. The first subcategory is traditional **Scams**, in which a stranger uses deception to trick someone out of his or her money. It might be the “grandparent scam,” where an older adult receives a late-night phone call from a caller who says, “Grandma? It’s me, your favorite grandson. I need your help. I’m traveling, and I was arrested. I need you to wire money to help me post bail. Please don’t tell mom or dad—they would be really upset!” Typically these requests are for a few thousand dollars, but we’ve seen people lose as much as \$70,000 over a series of increasingly high-pressure calls. It might be the “Nigerian prince” emails, or another con that requires an individual to make a payment to collect a lottery winning, insurance claim, government benefit, or grant. One “Australian lottery” victim lost threequarters of his life savings before mentioning the windfall he expected to receive to his daughter, who helped him realize he’d been conned. Or perhaps an offer to buy a senior’s car comes in the form of a cashier’s check that is \$2,000 over the agreed upon price. “No problem,” says the buyer. “Just send me back a check for the difference.”

We estimate that these scams cost American seniors \$9.85 billion per year. 43.9% of our sample indicated that an example of this type of fraud had been attempted over the last five years,²⁴ and 8.4% lost money to it. The mean five-year financial loss for someone who lost money to con artistry was \$13,225, with half of all victims losing \$2,500 or more.

The second subcategory of criminal fraud is **Identity theft**, which includes when someone takes out a credit card or other financial instrument in someone else’s name, using misappropriated information about his or her identity, or uses an existing financial product, such as a stolen credit card number or checkbook, without authorization.

Only 4.3% of our respondents lost money to identity theft, losing an average of \$7,633 over the five-year study period. We estimate that identity theft costs seniors \$2.91 billion per year, of which approximately \$773 million is lost to card fraud and check forgery. The remaining \$2.14 billion is lost to people opening new accounts or taking out new loans using stolen personal information.

Criminal Fraud

Examples

Con Artists

- Grandparent scam
- Nigerian prince emails
- Fake lottery winnings or government grants
- Sweetheart scam

Identity Theft

- Opening new credit cards, bank accounts, or payday loans
- Car title or home equity loans on your property
- Using card data gained by phishing, in data breach, or from the mail

Caregiver abuse

We included **Caregiver abuse** as a second category separate from fraud. Both kinds of abuse are illegal, but while fraud is enabled by anonymity, caregiver abuse is enabled by a trusting relationship with the victim.

The perpetrator is often a family member but can also be a paid caregiver, longtime friend, lawyer, accountant, financial manager, or someone else with an obligation of good faith to the victim. This cast of characters could range from the “helpful” son who visits every morning and asks to borrow \$100, knowing that by the next morning his mother with memory loss will have forgotten, to a paid caregiver who removes family heirlooms from the home for months before anyone notices, to the “friend” who just needs a “small loan” to get back on his feet.²⁵ Sometimes it occurs as hybrid financial abuse, a recently named category defined as financial abuse coupled with physical abuse or neglect that creates a fear or power dynamic that enables the abuse.²⁶

Other studies have reported that the majority of fraud is perpetrated by family members or paid caregivers.²⁷ At \$6.67 billion dollars, the amount of money our study identifies as lost each year to caregiver abuse is even larger than the amount identified by prior research. Importantly, the amount lost due to family member or

trusted party theft is on average larger than losses incurred through other types of abuse. The amount stolen by an errant nephew taking out an unauthorized mortgage is necessarily larger than the amount added as a shipping-and-handling charge for a TV purchase.

Our public policy needs to acknowledge, honor, and empower the family caregiver.

However, incidents involving family or other trusted parties occur in a much smaller percentage of respondents than incidents involving strangers or businesses. Focusing exclusively on caregiver abuse can obscure issues related to parties not in a position of trust.

It's important to recognize this because when attempting to resolve a situation of financial vulnerability, the solution is almost always either to "empower the caregiver" or to "disempower the caregiver." In other words, if a person is engaging in activity that is causing financial self-harm, he or she may need support to address the problem; the appropriate response is to find a trusted party and ask for his or her help. By contrast, if a caregiver is causing financial harm, the solution is to get him or her out of the picture.

Our public policy in situations of elder financial abuse often results in *removing* sources of support, rather than adding them. We believe that this can be damaging—that our public policy needs to acknowledge, honor, and empower the family caregiver. We estimate, for example, that merely by reviewing their parents' finances every few months, caregivers prevent 24,500 instances a year of financial fraud and exploitation that would have resulted in \$465 million of financial losses.²⁸

Caregiver Abuse

Examples

- Theft by family members or caregivers
- Rewritten wills or powers of attorney
- Borrowing money hoping senior will forget
- Sometimes combined with physical abuse or neglect

Financial exploitation

In contrast to criminal fraud and caregiver abuse, our third category, **Exploitation**, is defined as someone engaging in abusive action openly, expecting to avoid law enforcement actions on technicalities. This is behavior that relies on misrepresentations that are just within the bounds of the law and takes advantage of a person's vulnerability or confusion.²⁹ Such exploitation might be perpetrated by a U.S. corporation with a listed address and identifiable brand. Rather than operating under the radar, these organizations advertise on TV, bank at mainstream financial institutions, raise capital from legitimate financial markets, hire sales performance consultants to maximize their revenue, and so on.³⁰

Exploitation is frequently connected to products sold on TV, by phone, or in the mail. Typical examples might be a product that has an unexpected shipping-and-handling charge, includes a free trial that is hard to cancel, or is unexpectedly bundled with a subscription service.³¹ Another category includes services that are misrepresented in their marketing with smallfont disclaimers, such as creams that purport to help you lose weight, credit score improvement services, or work-from-home kits that require an upfront payment of several thousand dollars to help you set up your own "online store" to sell secondhand jewelry on eBay.

We believe it is critical to highlight this predatory activity, particularly when law enforcement is hesitant to bring ambiguous cases to court and journalists fall silent about crime that occurs in these gray areas. If a person reports a Nigerian phishing email in the press, the fraudster is not going to demand a correction or sue for libel. Nevertheless, we found that many people shied away from reporting the illegal practices of established, U.S.-based businesses. Put simply, they are getting away with it.

We estimate that financial exploitation costs seniors a startling \$16.99 billion a year. Victims in our study lost an average of \$2,716 over the course of five years to exploitative practices, with over half losing \$500 or more. 11% reported losing over \$5,000, and 4% reported losing over \$10,000. One survey respondent reported, "Mom exhausted her

Put simply, they are getting away with it.

savings. Now there is nothing to steal.” Often, this was the result of a piling-up of small things—“death by a thousand cuts,” as another respondent put it. These cases involved varying degrees of entrapment. Although the victim acted “voluntarily”—giving out a credit card number or sending a check—he or she was being deliberately setup to make a spending mistake. Typically, the closer we looked, the more obvious it became that the set-up was deliberate. For example, a company that sells a subscription service might use scoring techniques when buying lists of prospective customers from another subscription service vendor. While this kind of company might claim ignorance that the list it purchased primarily includes people with memory loss who forgot to cancel previous subscriptions, our interviews with call center representatives and reviews of sales scripts and training materials debunk such claims of ignorance. Based on our investigation of the industry, what’s going on within these organizations is an open secret, and it is clear they are systematically engaging in fraud.

Based on our investigation of the industry, what’s going on within these organizations is an open secret

Imagine this: A third-party marketing firm sends a senior with memory loss three free issues of a popular national magazine. The firm calls the senior and says, “You’ve been receiving [this magazine], and you have not yet paid for your subscription. According to the terms of your offer, today is the final deadline to make a required payment, so please give me your credit card number now.” The key phrase is “according to the terms of your offer”—the senior believes he has agreed to these terms, perhaps due to trust, confusion, pressure, or memory loss, and so believes he owes money when in fact he does not. Typically these subscriptions will be for terms as long as three to five years and will be at prices that are far above market rates for the magazine in question.

Here’s another common example: When a senior donates \$10 to a new charity, it may seem innocuous—hardly deserving of the term “fraud.” But imagine a company operating a massive call center that has bought a “sucker list” of people who are known to always donate—perhaps because of memory loss or cognitive impairment.

This company calls the same senior multiple times a day, substituting in one rent-a-charity after another, taking a 90% cut and giving 10% to the charitable cause. Suddenly, a charitable solicitation begins to look more clearly like exploitation. As one survey respondent put it, “If non-profits are allowed to harass seniors, they should at least pay full postage.”

Financial Exploitation

Examples

- Hidden shipping and handling or subscriptions
- Work-from-home schemes
- Quack weight loss or dietary products
- Excessive gifts
- Misleading financial advice

The financial exploitation progression

We also found that financial exploitation is rarely an isolated incident. Although the losses were small relative to other types of abuse—on average \$2,617 over a five-year period—we found that a senior who loses as little as \$100 over five years to petty exploitation is expected to lose \$9,660 to other types of fraud over the same five-year period. In other words, the loss of around \$20 a year can be seen as an indicator of an expected loss of around \$2,000 a year.³³

The takeaway is that *any financial loss at all should be taken as a sign of an underlying vulnerability*. An important message in media, nonprofit, and government awareness campaigns must be that no loss is small enough that it's safe to ignore.

A senior who loses as little as \$100 over five years to petty exploitation is expected to lose \$9,660 to other types of fraud.

Summary: Categories of Abuse			
Category	Who they are	What they do	How they hope to get away with it
Criminal fraud	Criminals	Trick seniors into sending money or providing personal information	Try not to get caught by operating anonymously
Exploitation	Businesses, charities, or individuals	Use pressure tactics or misleading language to lead seniors into financial mistakes	Because they technically did not lie or steal, they claim the senior acted voluntarily
Caregiver abuse	Family, friends, or paid helpers	Take advantage of the trust relationship to get money from the senior	Conceal the activity, or use intimidation or neglect to keep the senior silent

Non-financial effects of financial abuse

While the financial effects of elder abuse grab headlines, the non-financial effects are important as well.³⁴ Of the seniors who experienced fraud, 1.8% lost their home or other major assets as a result. 6.7% skipped medical care, and 4.2% reduced their nutritional intake for budgetary reasons. We estimate that 954,000 seniors are currently skipping meals as a result of financial abuse. Many suffered depression, anxiety, or loss of independence. Overall, 41.2% reported that financial abuse had nonfinancial costs as well.

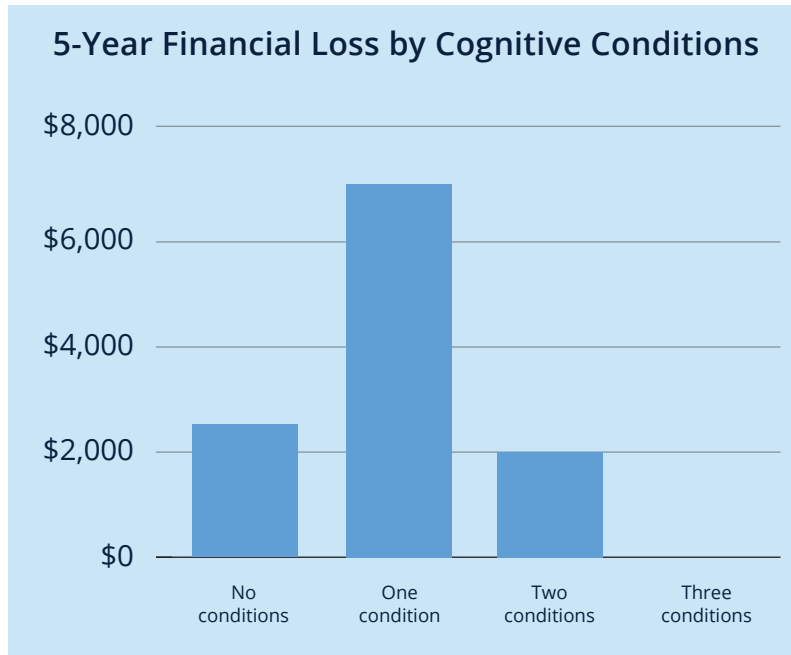
For the caregivers, the costs were also significant. Of all caregivers whose family member or care recipient experienced loss due to financial abuse, 27.9% reported

We estimate that 954,000 seniors are currently skipping meals as a result of financial abuse.

depression, stress, or anxiety stemming from dealing with the financial loss; 18.2% reported increased conflict with family and friends; and 13.9% reported a sense of hopelessness. Additionally, 7.3% experienced loss of career advancement or decreased hours at work, and 9.1% experienced damage to their marriage or romantic partnership. Given that 44 million Americans care for older adults,³⁵ these figures imply that 1.4 million marriages were damaged by the effects of dealing with fraud targeting parents or other loved ones over the study period, and 1.1 million caregivers' careers were set back because of hours away from work.³⁶

Risk factors

Our analysis revealed relationships between vulnerability and certain personal, medical, and socio-economic factors. Cognitive conditions that one would expect increase vulnerability do just that, while other factors that increase vulnerability are quite surprising. Perhaps most surprising are the factors that don't enhance vulnerability, especially where popular perception has previously suggested that they do.

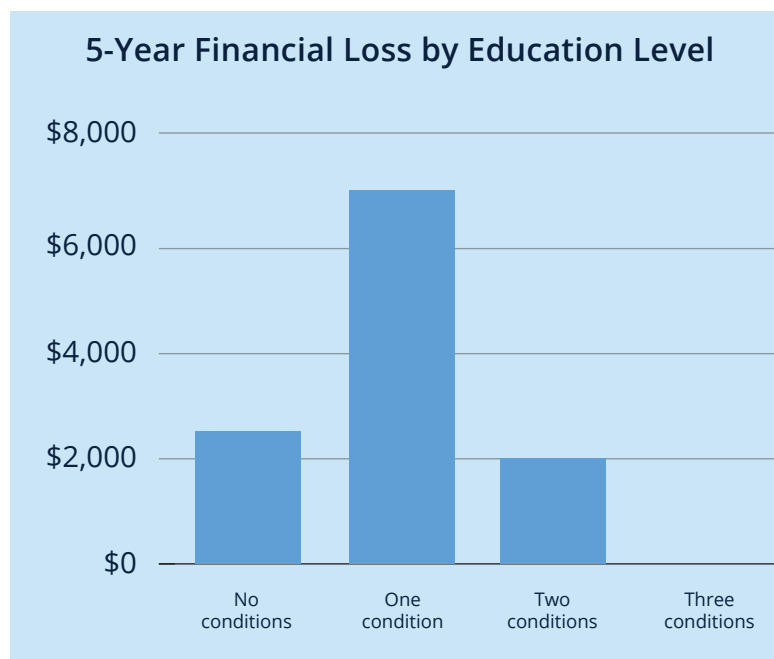


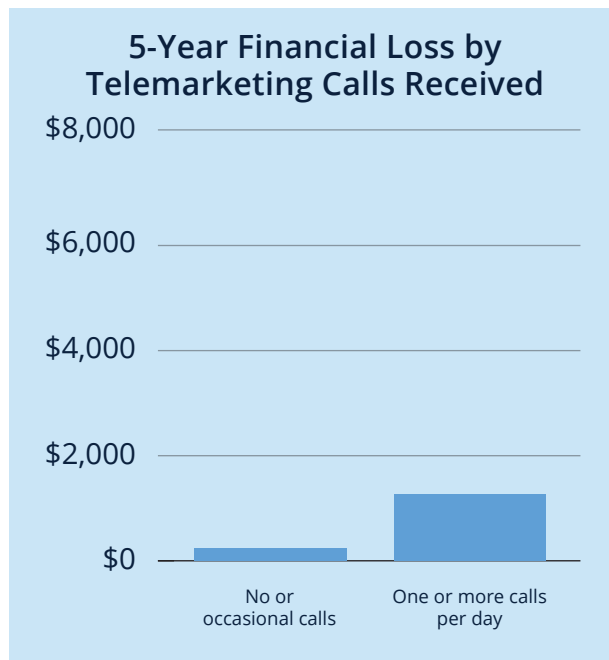
Unsurprisingly, memory loss is significantly associated with financial loss³⁷—both in likelihood of occurrence and in the amount lost. People with a below-average memory³⁸ are 78% more likely to suffer financial abuse and lost over twice as much.³⁹

Likewise, cognitive conditions such as dementia and Alzheimer's disease increase vulnerability.⁴⁰ People with one cognitive condition experience more financial loss from financial abuse than those with two or more conditions, presumably due to the fact that those with multiple conditions experience reduced independence. Stroke victims experience the greatest amount of financial loss, perhaps because the change is sudden and so there is less time to prepare for altered cognitive capabilities than in cases of dementia or Alzheimer's.

More unexpectedly, we found a significant relationship between how friendly a person was over the course of his or her life, and the amount of money lost. We call it "friendly grandma syndrome." You tell mom to hang up on telemarketers, but she is just too polite to hang up on anyone, and before you know it, she's ready to bake them cookies. In fact, someone described as "extremely friendly" over the course of his or her life is likely to experience four times the financial losses as someone with a more typical level of friendliness. One explanation for why friendliness leads to this kind of financial loss is that it increases exposure to more actors with abusive intentions. This theory is consistent with research that shows that age-related changes in cognition may increase vulnerability to fraud in a range of ways. Compared

with younger adults, older adults don't perceive cues of untrustworthiness as clearly;⁴¹ are more likely to be persuaded by information in advertisements;⁴² and experience subtle declines in judgment.⁴³ The research suggests that as you grow older your natural





alarm bells aren't set off as easily, and because friendly people are more outgoing, they may be exposed to more situations where alarm bells are needed.

Our study found education to be *positively* correlated with incidence of financial abuse. People with more education are more likely to be defrauded and tend to lose more money than others when this occurs. Financial sophistication had a more complex relationship to

incidence of financial abuse. People who are very financially sophisticated are likely to avoid certain types of financial loss, but the losses are bigger when they do fall victim, perhaps because they are more confident in their decision-making or more comfortable moving large amounts of money.⁴⁴ Ironically, these factors—being financially sophisticated and well educated—might give seniors a sense of complacency that actually increases their vulnerability. Previous research has shown that overconfidence in your own ability to manage money was as dangerous as memory loss in enabling fraud, and that even something as simple as whether or not you believe that seniors are often targeted by con artists is a predictor of whether you yourself will be targeted.⁴⁵ Additionally, people who live in urban areas experience more fraud and lose more money than people who reported living in rural areas.

People who receive calls from telemarketers are substantially more likely to experience fraud. A person who receives one phone call or more per day from a telemarketer is likely to experience three times as much financial loss as someone who receives no or only occasional telemarketing calls.⁴⁶

A person who receives one phone call or more a day from a telemarketer is likely to experience three times as much financial loss.

We did not find a relationship between gender and vulnerability. 36% of the women in our study and 35% of the men in our study lost money to elder financial abuse, with men losing slightly more in total.⁴⁷ Likewise, we did not find that people who are widowed are more vulnerable than people who are married or living with a partner. In fact, widowed people experienced about 8% less fraud. We did not find any support for the common stereotype that women are more vulnerable to making bad financial decisions. We also did not find that people who live farther away from their loved ones are exposed to greater risk of elder financial abuse.⁴⁸

We did not find a relationship between current household income or peak (i.e., pre-retirement) household income and probability of financial loss; however, the lowest-income people lose more on average due to slightly higher losses per incident.⁴⁹

We found that scam victimization followed a bimodal distribution with respect to age, with incidence peaking first around 60–65 and then again around 85 years old. This result is consistent with other studies, which find that among the types of fraud that affect older adults, the younger people within that category are most vulnerable to some types and the older people are most vulnerable to others.⁵⁰ For example, people under 70 lose over five times what the rest of the population lose to exploitation that revolves around the “fine print,” such as unexpected recurring billing or unwanted magazine subscriptions. People aged 85–90 lose almost five times as much as the rest of the population to problems stemming from too much generosity, such as unaffordable charitable contributions or gifts to family members or caretakers. We did find a positive but not significant relationship between having no children and experiencing financial abuse, and similarly between watching large amounts of television and experiencing financial abuse.

A history of thrift helps, but only within limits. People who disregarded budgeting—“not thrifty at all”—are more likely to lose money than those who don’t. But in some categories, extremely thrifty people see greater financial losses, perhaps because bargain-hunting is a behavior that scammers prey upon. An ideal disposition seems to be “spend what you can afford”—that is, being neither a shopaholic nor an extreme bargain-hunter.

These factors together tell a complex story about what makes an older adult susceptible. We can start by throwing out the stereotypes.

Rich or poor, male or female, widowed or married, we are all vulnerable.⁵¹ So what *does* cause vulnerability? On the one hand, people with memory loss or other “signs of aging” are more susceptible based on our findings. On the other hand, people who are younger, better educated, and more financially sophisticated are also vulnerable.

We conclude that increased risk arises at the intersection of the two sets of factors: *risk equals vulnerability plus exposure*. Older adults with independent, active lifestyles have more to be concerned about because they inadvertently provide perpetrators with more ways to target them.

Risk equals vulnerability plus exposure.

Factors that increase risk

Examples

- Cognitive conditions including dementia and Alzheimer’s disease
- College or graduate-level education
- Financial sophistication
- Friendliness
- Urban dwelling
- Poor memory
- Calls from telemarketers

Reporting and underreporting

The 2010 National Public Survey on White Collar Crime found that half of fraud victims reported the fraud, but only one in five reported it to law enforcement. The other four out of five cases were typically reported to banks and credit card companies to try to recoup the loss, or to the Better Business Bureau.⁵²

Likewise, a Financial Fraud Research Center study estimated that only one in thirty incidents of scams end up in a government database.⁵³

Typically, victims do not know to whom they should report the fraud, feel that reporting is likely to be useless, or are ashamed about having been duped.⁵⁴

Other victims may not report incidents because they hold onto hope that they'll get their money back (or what they were promised), or they fear retaliation.⁵⁵

Other research has shown that older adults are less likely both to acknowledge and to report that they've been taken advantage of.⁵⁶ The exceptions are illustrative: card fraud, check fraud, and identity theft are reported 80% of the time, because in such cases it's clear exactly whom to call, and that if you successfully make your case you'll get your money back. Other types of abuse are typically reported only 30% of the time.⁵⁷

Among our respondents, 29% of people who lost money to financial abuse stated that they had reported it to banks, police, or another government authority, while 71% stated that they had not made a report. The likelihood of reporting increased with the amount in question: 33% of people who lost over \$1,000 and 58% of people who lost over \$10,000 reported the losses.



Conclusion

The data about elder financial abuse speaks loudly. Criminal fraud, financial exploitation, and caregiver abuse cost older Americans more than \$36 billion a year, and that doesn't account for the profound emotional and physical costs to seniors and their families that we're just beginning to quantify.

This once-silent issue is beginning to get the attention it deserves. We hope these findings are a resource for the practitioners, policymakers, and press working to prevent elder financial abuse. We also hope this research can help us all to see the problem more clearly, in all its complexity. This is another step on the path to debunking the notion that the victims or the perpetrators of elder financial abuse fall into neat definitions that allow for simplistic solutions.

Whether by showing that those with more education are more likely to fall victim, or that mainstream corporations are as guilty of exploitation as illegal actors, or that the sheer size of the problem dwarfs previous estimates, what the data proves is that this is an issue we can't afford to ignore.



Appendix A: Common Examples

The Australian Lottery

A senior receives a phone call or email telling him that he's won the Australian lottery. In order to collect the winnings, he needs to pay import duties to clear customs, pay to insure the envelope containing the winnings, or pay a travel agent to arrange transportation so that he can collect the winnings in person. The senior is instructed to wire money or send Green Dot cards to the scammers.

The Blessing Scam

The Blessing Scam, also called the Ghost Scam or the Jewelry Scam, is a confidence trick typically perpetrated against elderly women in Chinatowns and overseas Chinese communities. The object of the scam is to persuade the victim to put valuables into a bag so that they can be blessed. Once this is done, the perpetrator secretly swaps the bag for a look-alike, thereby stealing the valuables. This scam takes advantage of Chinese and Chinese-American cultural traditions.

The Buyer's Club

A senior is offered an extremely low-priced cruise, but told she must enroll in a free trial of a buyer's club to qualify for the cruise and other offers. She believes that the free trial will end automatically, but in fact, her credit card number has been shared with the buyer's club, which begins billing her almost immediately. The senior is then charged a monthly membership fee, regardless of whether she uses any of the offers.

The Deathbed Scam

A terminally ill patient with life insurance is persuaded to sell the benefit of his policy for pennies on the dollar. Technically, this "viatical settlement" can be a legitimate transaction, as when a person uses the funds to pay for medical expenses he

wouldn't otherwise be able to afford. However, individuals peddling this type of settlement often take advantage of seniors who may feel like they have no other options or are led to believe they are getting a good deal. The payout amount is often far below the true value of the policy, and once the individual passes away, relatives and loved ones are unable to collect benefits and are left without recourse.

The Cemetery Scam

A senior preemptively pays for a cemetery plot in order to lift this responsibility from her family. When the senior passes away, it turns out that the plot doesn't actually exist or is worth much less than the senior paid. Alternatively, the family isn't made aware of the prior arrangement and buys an additional cemetery plot.

Counterfeit Prescription Drugs

Prescription drugs are often expensive. To find a better deal for medications, seniors may shop online, or via phone or mail. In the Counterfeit Prescription Drug Scam, the drugs sold are old or expired, or simply not what they are said to be. Fake botox and sexual aids are especially common, given some seniors' reluctance to request these items from their doctors.

The Disaster Scam

Immediately after disaster strikes, scammers set up fake websites or send out charity mailings to collect donations. For example, salvationarmyonline.org is not the real site of the Salvation Army, but in the days after Hurricane Katrina, it collected almost \$50,000 in donations before it was shut down. In the Disaster Scam, scammers not only take advantage of the generosity of seniors, but they also deprive those who are needy from receiving assistance.

The Fake Insurance Policy

An insurance broker collects monthly premiums for a fake policy and provides forged documents to the purchaser. When a problem arises and the insured individual attempts to collect benefits, the policy—and the broker—evaporate, leaving the victim financially unprotected. Insurance policies are complex and difficult to verify, making this scam all the more tricky.

The “Four For the Price of One” Scam

A senior citizen sees a TV commercial for a new kind of vacuum cleaner and calls the 1-800 number provided. The salesperson offers her four for the price of one, and fails to remind her of the fine print—the \$30 shipping-and-handling fee per item. The senior ends up being charged \$120 in shipping-and-handling alone, which is much more than she expected to pay for the \$40 vacuum cleaner. This scam operates under the assumption that the person buying the product will see the “four for the price of one” tagline and miss the fine print, including shipping-andhandling costs that are rarely refundable.

“Skimming” Scams

An employee at a retail store asks a senior for her credit card, and then “skims” the card to receive payment. What the senior doesn’t realize is that the employee has used a device to illegally copy the card’s information. This information can then be used to make unauthorized purchases. Skimming can occur at insecure ATM machines, gas pumps, and cash registers.

The Gift Basket Scam

The doorbell rings and a senior is presented with a lovely gift basket including a bottle of wine. Because the package contains alcohol, the senior needs to show a photo ID and pay \$2.50 to confirm receipt of the package.



The delivery person then requires payment by credit or debit card, thereby collecting personal account information. Within a few hours, the scammers have racked up thousands of dollars of charges online.

Grandparent Scam

A scammer calls pretending to be a grandchild in need of immediate funds. He states that he has “been arrested” while traveling. The caller asks for the money to be sent via wire and begs the grandparent not to tell his parents. The Grandparent Scam often happens late at night when a senior is groggy and easily confused. Increasingly, scammers are following actual grandchildren on social media so that they can provide real names and details to unknowing victims.

Hearing Aid Scam

A hearing aid vendor sets up at a mall or distributes a mailer offering a free hearing evaluation. Because everyone has technically suffered at least some level of hearing loss—nobody’s hearing is perfect—the salesperson, who appears to be a doctor or nurse, can truthfully say that a given senior has limited hearing ability. The vendor then says that a specific type of expensive hearing aid—often costing five to ten thousand dollars—is necessary to improve the condition. If the hearing aid is custom made, a no-returns policy will apply.

Helpful Nephew Scam

A senior’s family member or paid caregiver visits every morning to help with basic needs. Each day, he asks to borrow \$100, knowing that by the next morning the senior will have forgotten. A senior with memory loss will trust this individual, given that he is familiar and appears to be acting in good faith.



Home Improvement Scam

A scam home repair or improvement contractor contacts a senior and says he is ready to come and install a new air conditioner. He just needs credit card information to run the payment and then the installation can be scheduled. Not remembering whether she ordered an air conditioner or not, the senior goes ahead and pays for it. In other cases, a senior may have a genuine repair need, and an unscrupulous vendor will either over-charge, charge multiple times for the same work, or charge for work that isn't actually completed. In other variations of this scam, a person might go door-to-door offering to re-pave driveways for a low price, and then spend a half-hour dumping a bucket of concrete on the driveway or disappear without ever doing the work.

Immigration Scam

An "immigration lawyer" contacts a senior offering to adjust his immigration status and requests a fee that is required by a government agency in order to complete the documentation. The "lawyer" tells the senior that he will be in violation of the new status rules without this payment. While details may vary, all versions of the Immigration Scam involve a short or rushed deadline. Additionally, scammers follow major news stories about changes in immigration rules, in order to add legitimacy to their claims.

The Investment Scam

An ad or a salesman convinces a senior that some unusual asset—commemorative gold coins, a horse rescue farm, penny stocks—are a great investment vehicle, and then transfers substantial savings to the vendor or advisor to complete the purchase. Often, the investments are peddled door-to-door or through seminars in which co-conspirators are planted in the audience to talk about "how amazing" the deal has been for them.

Magazine Subscription Renewal Scam

A company sends three free issues of a magazine to a senior and then calls to say that according to the terms of the offer, today is the final deadline to pay for the subscription. What the caller says is true—it is the final deadline to extend the subscription—but the senior incorrectly believes he is required to pay or that he already owes money.

Medicare Card Scam

A caller tells a senior that he needs to renew his Medicare card, and asks the senior to provide the number on the front of his card. The caller then uses this information, which is the senior's Social Security number, to steal the senior's identity and open a credit card under his name. Government services—and especially those that primarily serve seniors—often have impostor callers requesting either information or money from unknowing victims.

Medicare Billing Scam

A senior is persuaded to undergo unnecessary medical treatment, and then Medicare is billed for the expense. Inappropriate Medicare billing costs the government billions in tax dollars, but more important, victims of this scam endure unwarranted medical treatments that may have other risks or cause health problems.

Missing Children Scam

A caller tells a senior that if she donates money to an organization supporting families of missing children, every dollar will go directly to the families in need. The scam here is in the word “directly;” if the senior donates over the phone, the funds will go through a paid telemarketing firm that takes as much as a 90% cut.

The Obituary Scam

Scammers troll the obituary sections of small-town newspapers looking for recent deaths that leave behind surviving partners. They will then call a widow and claim that her deceased husband actually owes thousands of dollars in unpaid debt. They will threaten financial ruin, eviction, and public shaming unless the debt is quickly paid. Often, a steeply discounted “settlement offer” is proposed if the debt is paid within a narrow time period.

Online Dating Con

Scammers contact a recently widowed senior online and quickly become a new “friend.” The scammer will generally play along for a while before he starts asking for money. Maybe he wants to come visit but cannot afford the flight; maybe he needs to clear a debt; or maybe he wants to help out a dear relative. The money is often requested in un-traceable ways, like a money order or a single-use prepaid card.

Pump and Dump Scams

A scammer buys inexpensive stock in a company (called “penny stocks”) and then artificially “pumps” up the value of the company by distributing false or misleading information—often via online banner ads promising investing tips. An internet campaign spreads false information across multiple sites making it difficult to verify the underlying details. At the peak stock price, the scammer then “dumps” the shares, selling them and leaving everyone else owning now worthless junk shares.

Religious Organization Scams

A suspect religious organization or scammer pretending to be a reputable place of worship will convince a senior to donate money to its cause. Later, the organization will quietly pressure the senior to rewrite his will. The rewritten will is often left undiscovered until after the senior’s death.

Sweepstakes Scam

A senior is told he has won a sweepstakes and needs to pay a small shipping-and-handling fee to collect his winnings. While the prize is visually represented as a new car or a cruise, the fine print indicates that prizes may vary. After paying a hefty fee, it turns out the senior has won a worthless trinket. The scam uses high-pressure language that preys on a senior's desire to help his family. "How will you feel," the solicitation asks, "when you have to explain to your family that you could have won \$50,000 but you passed up your chance?"

Sweetheart Scam

A younger man or woman befriends an older adult and creates a very close relationship with the senior. The goal of this scheme is to be written into the senior's will, or to be given money directly. This scam targets lonely seniors who have become isolated due to health issues or the loss of their friends and loved ones.

Telemarketing Scams

Predatory telemarketers contact vulnerable seniors to access their personal or financial information. They may use emotional appeals like guilt, friendliness, or scapegoating to encourage the senior to provide information. The scripts used by these telemarketers are data-driven and designed to be extremely persuasive. The companies then sell the information to other telemarketers using the same tactics, leading to an unstoppable onslaught of telemarketing calls.

The Veterans Scam

A senior citizen gets a call asking for money to help families of military veterans. The senior is told that she has supported this cause in the past. While this may be true in a more general sense, the caller leads the senior to believe that she has supported that specific organization. The senior then feels more comfortable donating "again."

Weight Loss Magnets

It sounds too strange to be true, but magnets that allegedly lead to weight loss is one of the top scams reported by the FTC. All sorts of anti-aging, beauty, or weight-loss treatments are hawked on TV, often as subscriptions or “free” trials. There is no evidence that any of these treatments—including magnets—help with weight loss.

Work-From-Home Scams

A senior purchases a kit to start a small business, such as an online store to sell vintage jewelry or health supplements. After an expensive set-up fee, hosting fee, and initial stock of jewelry, few buyers visit the online store. The senior is then told she isn’t promoting the store hard enough and is encouraged to pay money for “business coaching.” Even worse, Work-From-Home Scams are often pyramid schemes, where victims get paid to recruit others into the scheme.



Appendix B: Significant Risk Factors

Vulnerability factors and results			
Factor	Value	Impact	Comparison values
Condition that could limit decision-making capacity	<ul style="list-style-type: none"> • At least 1 	<ul style="list-style-type: none"> • 59% more likely 	<ul style="list-style-type: none"> • Less than 1
Education	<ul style="list-style-type: none"> • College study or degree • Graduate study or degree 	<ul style="list-style-type: none"> • Lose 3 to 5 times as much 	<ul style="list-style-type: none"> • Less than high school • High school
Financial sophistication	<ul style="list-style-type: none"> • Very sophisticated • Extremely sophisticated 	<ul style="list-style-type: none"> • Lose twice as much 	<ul style="list-style-type: none"> • Moderately sophisticated • Slightly sophisticated • Not sophisticated
Friendliness	<ul style="list-style-type: none"> • Extremely friendly 	<ul style="list-style-type: none"> • Lose 4 times as much 	<ul style="list-style-type: none"> • Very friendly • Moderately friendly • Slightly friendly • Not friendly at all
Gender	<ul style="list-style-type: none"> • Female 	<ul style="list-style-type: none"> • <2% more likely 	<ul style="list-style-type: none"> • Male
Location type	<ul style="list-style-type: none"> • Urban 	<ul style="list-style-type: none"> • 47% more likely • Lose 4 times as much 	<ul style="list-style-type: none"> • Rural
Marital status	<ul style="list-style-type: none"> • Widowed 	<ul style="list-style-type: none"> • <8% more likely 	<ul style="list-style-type: none"> • Divorced • Never married • Married or living with a partner
Memory	<ul style="list-style-type: none"> • Poor or fair 	<ul style="list-style-type: none"> • 78% more likely • Lose 2 times as much 	<ul style="list-style-type: none"> • Good • Very good • Excellent
Receives calls from telemarketers	<ul style="list-style-type: none"> • One or more telemarketing calls per day 	<ul style="list-style-type: none"> • Lose 4 times as much 	<ul style="list-style-type: none"> • No calls • Only occasional
Stroke	<ul style="list-style-type: none"> • Had a stroke 	<ul style="list-style-type: none"> • Lose 5 times as much 	<ul style="list-style-type: none"> • Have not had a stroke
Thrift	<ul style="list-style-type: none"> • Extremely thrifty 	<ul style="list-style-type: none"> • Lose 5 times as much 	<ul style="list-style-type: none"> • Very thrifty • Moderately thrifty • Slightly thrifty • Not thrifty at all
Thrift	<ul style="list-style-type: none"> • Not thrifty at all • Slightly thrifty 	<ul style="list-style-type: none"> • 70% more likely 	<ul style="list-style-type: none"> • Extremely thrifty • Very thrifty • Moderately thrifty

Endnotes

1. We did not consider inappropriate financial products within the scope of this study, although they pose another increasingly prevalent problem. Commission-based sales reps might recommend, for example, a high-fees investment vehicle or a high-interest personal loan or home equity line of credit. We did not include these products because they were difficult to measure: one would need a detailed picture of an individual's financial situation in order to determine which financial products are, in fact, appropriate, and even then in many cases this would remain a judgment call.
2. This total includes \$60 million of reported financial losses for which we could not determine the appropriate subcategory.
3. This report uses the terms "senior" and "older adult" interchangeably to refer to people over 65 years of age. "Elder financial abuse" and "senior financial abuse" are also used interchangeably to refer to any time someone took financial advantage of an older adult in a that would not have been possible when the person was younger.
4. See the U.S. Federal Trade Commission report by Deborah Platt Majoras et al., *The FTC in 2007: A Champion for Consumers and Competition* (Washington, DC: FTC, 2007), http://www.ftc.gov/sites/default/files/documents/reports_reports_annual/annual-report-2007/chairmansreport2007_0.pdf; and Richard M. Titus et al., "Victimization of Persons by Fraud," *Crime & Delinquency* 41.1 (1995): 54–72; John Kane et al. *The 2005 National Public Survey on White Collar Crime* (National White Collar Crime Center 2006), <http://fraudresearchcenter.org/wp-content/uploads/2012/02/NWCCC-2005-national-public-household-survey.pdf>, and Rodney Huff et al., *The 2010 National Public Survey on White Collar Crime* (National White Collar Crime Center 2006), <http://www.nw3c.org/docs/publications/2010-national-public-survey-on-white-collar-crime.pdf?sfvrsn=8>; Jan van Dijk et al., *Criminal Victimization in International Perspective* (The Hague: United Nations International Crime Victims Survey 2007), http://www.unicri.it/services/library_documentation/publications/icvs/publications/ICVS2004_05report.pdf. For a review of this research, see Martha Deevy, et al., "Scams, Schemes & Swindles: A Review of Consumer Financial Fraud Research" (Financial Fraud Research Center, 2012), <http://fraudresearchcenter.org/wp-content/uploads/2012/11/Scams-Schemes-Swindles-FINAL.pdf>, and Kristy Holtfreter, et al., "Financial Exploitation of the Elderly in a Consumer Context" (2014), <https://www.ncjrs.gov/pdffiles1/nij/grants/245388.pdf>, a report submitted to the US Department of Justice.
5. Two AARP studies found that adults over 50 accounted for 57% of all fraud victims and that the 50–64-year-old age cohort was the most likely group to report having

been victimized by a major fraud. See AARP *Telemarketing Fraud Victimization of Older Americans: An AARP Survey* (Washington, DC: Princeton Survey Research Associates, 1996) and *Consumer Behavior, Experiences and Attitudes: A Comparison by Age Groups* (Washington, DC: Princeton Survey Research Associates, 1999). Older adults are less likely to be internet users, and the FTC found that just over half of incidents of fraud occur online. For almost every type of fraud that occurs offline, though, seniors are more likely to be victimized. See Keith B. Anderson, *Consumer Fraud in the United States, 2011: The Third FTC Survey* (Washington, DC: Federal Trade Commission, 2013).

6. Shelley Taylor et al., "Neural and Behavioral Bases of Age Differences in Perceptions of Trust," *Proceedings of the National Academy of Sciences* 109.51 (2012) 20848-20852. See also Larry Jacoby, "Aging, Subjective Experience and Cognitive Control: Dramatic False Remembering by Older Adults," *Journal of Experimental Psychology* 134.2 (2005): 131-148, summarized in Beth Azar, "Memory Loss May Be Behind Older People's Susceptibility to Scams," *Monitor on Psychology* 32.11 (2001): 30. See also, Zachary Urbina, "Neuroscience Team Explains Why Old People Get Scammed," *United Academics* (December 4, 2012), <http://www.united-academics.org/magazine/mind-brain/neuroscience-team-explains-why-old-peopleget-scammed/>, and Richard C. Lewis, "Why Are Elderly Duped? Area in Brain Where Doubt Arises Changes With Age," *ScienceDaily* (August 16, 2012), <http://www.sciencedaily.com/releases/2012/08/120816121836.htm>.
7. See especially *The MetLife Study of Elder Financial Abuse: Crimes of Occasion, Desperation, and Predation Against America's Elders* (New York: Mature MetLife Market Institute, 2011), <https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf>, but also *Broken Trust: Elders, Family, and Finances* (New York: MetLife Market Institute, 2009), <https://www.metlife.com/assets/cao/mmi/publications/studies/mmi-study-broken-trustelders-family-finances.pdf>.
8. According to Lifespan of Greater Rochester, Inc. et al., *Under the Radar: New York State Elder Abuse Prevalence Study* (2011), <http://www.ocfs.state.ny.us/main/reports/Under%20the%20Radar%2005%2012%2011%20final%20report.pdf>, elder financial abuse in New York State occurs at a rate nearly 44 times greater than is reported.
9. Please see note 4 above for the relevant research.
10. House Committee on Government Operations, *The Nature and Extent of Telemarketing Fraud and Federal and State Law Enforcement Efforts to Combat It: Hearings Before the Commerce, Consumer and Monetary Affairs Subcommittee of the House Committee on Government Operations*, 101st Cong., 2d sess. July 11 and 12, 1990. See also the testimony of Charles L. Owens, then Chief of the FBI's Financial Crimes Section, and others in the Senate Special Committee on Aging, *Telescams Exposed: How*

Telemarketers Target the Elderly: Hearing Before the Special Committee on Aging, 104th Cong., 2d sess., March 6, 1996. In the hearing, the consensus was that telemarketing fraud was a \$40-billion problem. See Ultrascan's finding (2008) that \$4.3 billion were lost to advance fee fraud in 2006, reported in Stuart Ross and Russell G. Smith, "Risk Factors for Advance Fee Fraud Victimization," *Trends & Issues in Crime and Criminal Justice* 420 (2011), http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi420.pdf.

11. Also, according to the 2010 Investor Protection Trust (IPT) Elder Fraud Survey, "more than seven million older Americans—one out of every five citizens over the age of 65—already have been victimized by a financial swindle." See <http://www.investorprotection.org/protectyourself/?fa=protect-seniors>.
12. Rebecca Fettes, *The Financial Exploitation Data Book: A Retrospective Look At Community Based Financial Exploitation in Oregon in 2013* (OOAPI and Oregon Department of Human Services, 2014), <http://www.oregon.gov/dhs/spwpd/adult-abuse/Documents/Financial-Exploitation-Oregon.pdf>, 27, estimates that financial exploitation could cost older Oregonians \$439,257,487 per year.
13. Richard J. Bonnie and Robert B. Wallace, *Elder Mistreatment: Abuse, Neglect, and Exploitation in an Aging America* (Washington, DC: National Academies Press, 2003). The relevant appendix ("Analysis of Elder Abuse and Neglect Definitions Under State Law") is available at the NIH website at <http://www.ncbi.nlm.nih.gov/books/NBK98799/>.
14. This is an increasingly common description of elder financial abuse. One notable source of this characterization is the testimony of Sandra Timmermann, then Executive Director of the MetLife Mature Market Institute, before the Senate Special Committee on Aging, *Protecting Our Seniors: Supporting Efforts to End Elder Abuse: Field Hearing Before the Special Committee on Aging*, 112th Cong., 1st sess., August 23, 2011, <http://www.gpo.gov/fdsys/pkg/CHRG-112shrg70551/html/CHRG-112shrg70551.htm>.
15. Applied Research & Consulting LLC for FINRA, *Financial Fraud and Fraud Susceptibility in the United States: Research Report from a 2012 National Survey* (New York: FINRA Investor Education Foundation, 2013), http://www.finrafoundation.org/web/groups/sai/@sai/documents/sai_original_content/p337731.pdf?utm_source=MM&utm_medium=email&utm_campaign=Foundation_News_091213_FINAL. See also Michaela Beals, "The Impact of Survey Context on Self-Reported Rates of Fraud Victimization" (Fraud Research Center, 2014), <http://fraudresearchcenter.org/wp-content/uploads/2014/10/Fraud-Issue-Brief-FINAL-10.14.14.pdf>, for a discussion of how study context (e.g., "crime" or "fraud") impacts self-reporting of fraud victimization.

16. See Peter A. Lichtenberg et al., “Is Psychological Vulnerability Related to the Experience of Fraud in Older Adults?” *Clinical Gerontologist* 36.2 (2013): 132–146, for a helpful counterexample.
17. See Michael Ross et al., “Contrary to Psychological and Popular Opinion, There Is No Compelling Evidence That Older Adults Are Disproportionately Victimized by Consumer Fraud,” *Perspectives on Psychological Science* 9.4 (2014): 427–442.
18. See *Off the Hook: Reducing Participation in Telemarketing Fraud* (Washington, DC: 2003), http://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf. Research that focuses on internet fraud overwhelmingly finds that younger people are more vulnerable than elderly people, while research that focuses on abuse by family members and caregivers—unsurprisingly—finds that vulnerability increases steadily with age.
19. The respondents were 44% male and 56% female. Of the seniors whose finances they described, 31% had peak household income under \$50,000; 46% had peak household income between \$50,000 and \$100,000; and 23% had peak household income over \$100,000. 91% were high school graduates, and 30% had completed college.
20. See Martha Deevy and Michaela Beals, “The Scope of the Problem: An Overview of Fraud Prevalence Measurement” (2013), http://fraudresearchcenter.org/wp-content/uploads/2013/11/Scope-of-the-Problem-FINAL_corrected2.pdf and “The True Impact of Fraud: A Roundtable of Experts” (2014), <http://fraudresearchcenter.org/wp-content/uploads/2014/06/The-True-Impactof-Fraud-Proceedings-Final.pdf>.
21. We did not regard these transactions as representative of the general public, and so did not include this data in our statistical analysis. Likewise, we did not extrapolate from the experiences of the customers we interviewed to draw conclusions about the general public.
22. We used 44,574,166 as the number of people over 65 in the United States based on the Census QuickFacts July 1 2013 estimated total population and percent over 65. The American FactFinder estimate is 44,704,074, with the QuickFacts percentage likely calculated from this estimate and then rounded.

A more detailed discussion is beyond the scope of this study, but it would be natural to assume that fraud—like the costs of natural disasters—follows a Pareto or truncated Pareto distribution. This means that estimates of the size of the problem drawn from samples—even with samples of tens of thousands of individuals—will typically underestimate the population statistic. Within our data, exploration of “peaks over threshold” analysis and bootstrapped subsamples provided initial confirmation of this hypothesis.

For a more thorough treatment of this topic, see David Giles et al., “Bias-Corrected Maximum Likelihood Estimation of the Parameters of the Generalized Pareto Distribution,” (University of Victoria Department of Economics, Econometrics Working Paper EWP0902), http://web.uvic.ca/~dgiles/downloads/working_papers/ewp0902_revised.pdf. A fitting of our data put the alpha shape parameter less than one. In other words, the population total fraud loss is bounded in practice by the finite wealth of Americans (a finite sample of an unbounded-mean distribution), rather than by a property of the shape distribution. Our data are not extensive enough to justify exploration of the domain of support for fitting a Pareto distribution. Such data would be nearly impossible to gather.

23. Under the leadership of Senators Bill Nelson and Susan M. Collins, the United State’s Senate Special Committee on Aging has focused on addressing what they refer to as an “epidemic of fraud perpetrated against seniors.” In particular, in November 2013 they launched a fraud hotline that collected 1,900 complaints in its first year. See *Fighting Fraud: Lessons Learned from the Senate Aging Committee’s Consumer Hotline* (2014), <http://www.aging.senate.gov/imo/media/doc/Fraud%20Hotline%20Report%20Final%20Version.pdf>, for information about the most common kinds of fraud, including computer repair scams, the grandparent scam, health scams, lottery scams, social security fraud, timeshare scams, and guardianship abuse.
24. We asked each respondent to provide data about five years of financial impact. Please see the methodology section for further details.
25. There is some room for interpretation here. A gift to a friend or family member could be labeled as predatory exploitation or it might be labeled as caregiver abuse depending on the circumstance.
26. Shelly L. Jackson and Thomas L. Hafemesiter, *Financial Abuse of Elderly People vs. Other Forms of Elder Abuse: Assessing Their Dynamics, Risk Factors, and Society’s Response* (2010), <https://www.ncjrs.gov/pdffiles1/nij/grants/233613.pdf>, a report to the National Institute of Justice, summarized in “Financial Exploitation of the Elderly,” on the National Institute of Justice website, <http://www.nij.gov/topics/crime/elder-abuse/pages/financial-exploitation.aspx>.
27. The most recent study is “New Allianz Life Study Confirms Elder Financial Abuse Under-reported and Misunderstood Problem Likely to Grow” (October 15, 2014), <https://www.allianzlife.com/about/news-and-events/news-releases/Press-Release-October-15-2014>. We were unable to find a copy of the 2014 Safeguarding Our Seniors Study that the Allianz Life Study’s authors reference. The finding that most fraud is perpetrated by family and paid caregivers is typical of many other studies.

28. I.e., fraud resulting in a loss of \$25,000 or more. We looked only at major fraud here because caregivers who reported having never reviewed their parent's financial statements typically also did not report having noticed small unwanted charges, for obvious reasons.
29. In the survey data, there were some cases where the inappropriate spending was in the form of gifts. It was often difficult to classify whether this constituted caregiver abuse or exploitative sales. We distinguished between a voluntary action driven by confusion or vulnerability—a poor decision to make the gift—on the one hand, versus a power relationship, coercion, or deception used to extract the gift, on the other.
30. *The New York Times* has provided seminal coverage of the way mainstream financial institutions and publicly traded companies enable financial exploitation of the elderly. See Charles Duhigg, "Bilking the Elderly, with a Corporate Assist," *The New York Times* (May 20, 2007), <http://www.nytimes.com/2007/05/20/business/20tele.html>, and Jessica Silver-Greenberg, "Banks Seen as Aid in Fraud Against Older Consumers," *The New York Times* (June 10, 2013), <http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html>.
31. See Ron Shevlin, "The Economic Impact of Grey Charges on Debit and Credit Cardholders and Issuers: 2013 Industry Report on Grey Charges" (New York: BillGuard, 2013), https://s3.amazonaws.com/static.billguard.com/report/BillGuard_-_2013_Grey_Charge_Report.pdf, for an estimate of \$14.3 billion in grey charges. The sample population comprises users of the BillGuard mobile app, which may overestimate the extent of grey charges in that the audience has self-selected for concern about grey charges. On the other hand, this population may underestimate grey charges in that selecting for users of a mobile app may eliminate parts of the population with the highest levels of vulnerability.
32. See Duhigg, "Bilking the Elderly," for description of "sucker lists": "InfoUSA advertised lists of 'Elderly Opportunity Seekers,' 3.3 million older people 'looking for ways to make money,' and 'Suffering Seniors,' 4.7 million people with cancer or Alzheimer's disease. 'Oldies but Goodies' contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: 'These people are gullible. They want to believe that their luck can change.'" As one of the nation's leading experts on fraud, Doug Shadel of the AARP put it on *Dan Rather Reports*, "Never get started with it. When you get a piece of mail, for example, that says you might have won something, it isn't a benign act to respond to that. Because what you're doing when you respond to it, even if it's sending \$5 in, is you're telling the bad guy, I'm someone who does this. And you're separating yourself out from someone who does this, from someone who doesn't do this. That gets a big, red X on your back. And now, you're being targeted by the really bad guys." "Just Hang Up the Phone," *Dan Rather Reports*,

- Season 8 Episode 9, (March 12, 2013). In Marguerite DeLiema et al., "Tricks of the Trade: Motivating Sales Agents to Con Older Adults," *The Gerontologist* (2014,): 1–11, researchers show how common mass market sales tactics were tweaked and amplified to target and deceive vulnerable older adults via door-to-door sales by the Alliance for Mature Americans, which sold \$200 million in living trusts and annuities to Californians in the 1990s before being shut down for deceptive sales practices.
33. Keith Jacks Gamble et al. in "The Causes and Consequences of Financial Fraud Among Older Americans," *Center for Retirement Research at Boston College Working Papers* (November 2014), <http://crr.bc.edu/working-papers/the-causes-and-consequences-of-financial-fraud-amongolder-americans/>, infer a causal relationship here using propensity-matched multi-year panel data. In particular, people who experience fraud become more risk-accepting than they were previously. This is an effect commonly seen in gambling or investing where after taking losses the decision maker shows increased willingness to take on risk in an effort to break even.
 34. We are especially grateful to Martha Deevy and her coauthors for urging further study of this topic.
 35. National Alliance for Caregiving and AARP, *Caregiving in the U.S.* (New York: MetLife Foundation, 2009), http://www.caregiving.org/data/Caregiving_in_the_US_2009_full_report.pdf. See also the summaries on the Family Caregiver Alliance homepage, e.g. <https://www.caregiver.org/selected-caregiver-statistics>.
 36. Also notable, though outside the scope of the research covered in this report, are the financial and non-financial costs to society. When older adults lose their nest eggs or all their assets, they rely more heavily on public services. As Shawna Reeves, Director of Elder Abuse Prevention at the Institute on Aging, puts it, "taxpayers often have to foot the bill when a senior's life falls apart due to elder financial abuse." See Norma Paz García et al., *Examining Faulty Foundations in Today's Reverse Mortgages* (Consumers Union, CANHR, and Council on Aging Silicon Valley, 2010), <http://consumersunion.org/wp-content/uploads/2013/02/reverse-mortgagereport-2010.pdf>, for an example of this collateral cost to taxpayers resulting from the Reverse Mortgage industry.
 37. We use "significant" in this section to indicate 95% confidence. Most of the data here was categorical rather than numeric. We used three statistical measures where appropriate: linear regression for ordinal variables, regression with indicator variables for categorical variables lacking an ordinal interpretation, and difference-of-means t tests where the category values could logically be grouped. In drawing a conclusion, we generally looked both at the magnitude of losses and the probability of losses, and looked for monotonic effects, robustness across multiple formulations of the model, similar effects on variables that were substantively related, and extra sources of inference based on the types of fraud that occurred.

38. More precisely the 43% of the sample whose memory was rated “Fair” or “Poor” rather than “Good,” “Very Good,” or “Excellent”.
39. We looked at change in memory function, but did not find that this had a stronger predictive relationship than the state of memory function. One might guess that the most vulnerability occurs when memory issues are creeping up on an older adult, but we did not find evidence that this was the case. A declining memory was significantly related to incidence of fraud, but this washed out when current memory was included in the regression.
40. Kristen Triebel and Daniel Marson have also shown that declines in financial decision-making are an early sign of cognitive impairment. K. L. Triebel and D. C. Marson, “The Warning Signs of Diminished Financial Capacity in Older Adults,” *Generations* 36.2 (2012): 39–45, <http://generations.metapress.com/content/4174t21up3804772>.
41. Shelley Taylor, “Neural and Behavioral Bases of Age Differences in Perceptions of Trust.”
42. Diane M. Phillips, and John L. Stanton, “Age-Related Differences in Advertising: Recall and persuasion,” *Journal of Targeting, Measurement and Analysis for Marketing* 13 (2004): 7–20, <http://www.palgrave-journals.com/jt/journal/v13/n1/abs/5740128a.html>.
43. P.A. Boyle, et al., “Poor Decision-Making Is a Consequence of Cognitive Decline Among Older Persons without Alzheimer’s Disease or Mild Cognitive Impairment,” *PLoS ONE* 7.8 (2012): e43647, <http://www.ncbi.nlm.nih.gov/pubmed/22916287>; Natalie L. Denburg et al., “The Orbitofrontal Cortex, Real-World Decision Making, and Normal Aging”, *Annals of the New York Academy of Sciences* 1121 (2007): 480–498, <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2246008/>
44. This finding is consistent with the FINRA Investor Education Foundation’s finding that willingness to take risk with investments is positively correlated with education, household income and susceptibility to fraud, See FINRA, *Financial Fraud and Fraud Susceptibility in the United States*, and with Gamble et al., “The Causes and Consequences of Financial Fraud Among Older Americans,” which we believe has not yet gotten the attention it deserves. The latter study looks carefully at these questions and concludes: “We find that overconfidence is a significant risk factor for becoming a victim of financial fraud. A one standard deviation increase in overconfidence increases the odds of falling victim to fraud by 26 percent. Financial knowledge, not just general knowledge, protects against fraud: years of education is not a significant predictor of the likelihood of being victimized by fraud.”
45. Keith Jacks Gamble et al., “The Causes and Consequences of Financial Fraud Among Older Americans.”

46. Holtfreter, Reisig, and Pratt have shown that “remote-purchasing activities” (making a purchase from a telemarketer, tv infomercial, mailing or from someone with whom they have not previously done business) increase the likelihood of fraud victimization, given that these activities indicate greater “exposure to potential motivated offenders.” See Kristy Holtfreter et al., “Low Self-Control, Routine Activities, and Fraud Victimization,” *Criminology* 46.1 (2008): 189–220. http://www.academia.edu/738038/Low_self-control_routine_activities_and_fraud_victimization. Likewise, according to Holtfreter, Reisig, Mears and Wolfe, on self-report survey data, “Making a telemarketing purchase substantially increased targeting. Respondents who purchased something in response to a telemarketing call from a company with whom they had not previously done business during the previous year increased their risk of becoming a fraud target by over 200% compared to those who had not made such purchases.” See Kristy Holtfreter et al., “Financial Exploitation of the Elderly in a Consumer Context” (2014), 12, <https://www.ncjrs.gov/pdffiles1/nij/grants/245388.pdf>.
47. This is not to ignore the gender dimension. Any issue relating to aging is a gender equality issue because of the predominance of women among the older population—and this population’s caregivers.
48. In fact, seniors who lived more than an hour away from their caregivers experienced significantly less fraud than those who lived close by. It’s unclear how to draw a cause and effect relationship here. It may be that when parents start to falter they move closer to their children, or their children move closer to them.
49. The FTC’s *Consumer Fraud in the United States* reports similar findings about income, gender, and marital status.
50. Keith B. Anderson, *Consumer Fraud in the United States, 2011: The Third FTC Survey*.
51. AARP Foundation’s *Off the Hook: Reducing Participation in Telemarketing Fraud*, and Karla Pak and Doug Shadel, *National Fraud Victim Study* (Washington, DC: AARP, 2011), <http://assets.aarp.org/rgcenter/general/fraud-victims-11.pdf>, showed that the victims of different kinds of scams had dramatically different profiles. For example, investment fraud victims were more likely to be male, younger, and with relatively higher income, while lottery scam victims were more likely to be female (in 2003 study, not 2011), older, and relatively lower income.
52. Rodney Huff et al., *The 2010 National Public Survey On White Collar Crime*.
53. They note that fraud is under-reported to authorities by a factor of thirty. This means there are one million complaints for almost forty million incidents. See Deevy et al., “Scams, Schemes, & Swindles,” comparing two FTC studies. The article offers a number of useful ways to respond to underreporting.

54. FINRA, Financial Fraud and Fraud Susceptibility in the United States.
55. Debbie L. Deem, "Notes from the Field: Observations in Working with the Forgotten Victims of Personal Financial Crimes," *Journal of Elder Abuse & Neglect*, 12.2 (2000). Experts often encourage an altruistic appeal when trying to encourage a senior to report fraud. See Sid Kirchheimer, "Protect Your Parents From Scams: Here's How to Talk to Mom and Dad About Steering Clear of Fraudsters," AARP (August 20, 2013), <http://www.aarp.org/money/scamsfraud/info-08-2013/protect-your-parents-from-scams.html>.
56. Karla Pak and Doug Shadel, *National Fraud Victim Study*.
57. Rodney Huff et al., *The 2010 National Public Survey On White Collar Crime*.



True Link

True Link Financial

www.truelinkfinancial.com

© 2015 True Link Financial