

St. Cloud State University

The Repository at St. Cloud State

Culminating Projects in Criminal Justice

Department of Criminal Justice

5-2022

Elder Financial Exploitation and Scam Activities Targeting Elderly Victims

Nora Doyle

Follow this and additional works at: https://repository.stcloudstate.edu/cjs_etds

Recommended Citation

Doyle, Nora, "Elder Financial Exploitation and Scam Activities Targeting Elderly Victims" (2022).
Culminating Projects in Criminal Justice. 17.
https://repository.stcloudstate.edu/cjs_etds/17

This Thesis is brought to you for free and open access by the Department of Criminal Justice at The Repository at St. Cloud State. It has been accepted for inclusion in Culminating Projects in Criminal Justice by an authorized administrator of The Repository at St. Cloud State. For more information, please contact tdsteman@stcloudstate.edu.

Elder Financial Exploitation and Scam Activities Targeting Elderly Victims

by

Nora Doyle

A Thesis

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science

in Criminal Justice

May, 2022

Thesis Committee:
Lee Gilbertson, Chairperson
Shawn Williams
Phyllis Greenberg

Abstract

Elder Financial exploitation is being referred to as the “crime of the 21st century due to its yearly increase in losses and rate of victimization, with the estimated loss ranging from \$2.9 billion to \$36.5 billion annually. This research was conducted to better understand the type of scams that elders fall victim to, what is being done to help stop these crimes and assist elders, as well as the prevalence of victimization and limitations of current laws and legislation. This integrative research was conducted utilizing online databases and peer-reviewed research to obtain the relevant details of this thesis. Results from research using online methods revealed that the true scope of elder financial exploitation is not known. This is especially relevant in the amount of annual losses, as well as rates of victimization which indicate that only 1 in 24 cases of elder abuse are even reported.

Problem Statement

Elder Financial exploitation from scam related activities is a growing issue in the United States, costing our nation’s elders billions of dollars every year. Despite the intervention of federal and state government agencies and legislation, the number of victims and annual losses continues to rise at alarming rates. The manner in which the scam is played out is getting increasingly more sophisticated and grow with the times (i.e. charity scams). In this research, it is the author's intention to review the current information surrounding elder financial exploitation in scam related activities and shed light on current issues.

Table of Contents

	Page
List of Tables.....	5
Chapter	
I. Introduction	6
Operationalization of terms.....	6
Introduction	6
About the Author.....	7
Background and Need.....	7
Purpose of the Study	8
Research Questions	9
Methods	10
II. Literature Review	12
Introduction	12
What is Elder Financial Exploitation and Abuse	12
Who is an Elder? And What is Elder Financial Exploitation?	13
The Elder Individual as a Victim	14
The Introduction of Elder Financial Exploitation	15
Prevalence of Scam Related Activity and Financial Exploitation in the Elderly	24
Prevalence of Scam Related Activities	25
Prevalence of Scam and Fraud Related Elder Financial Exploitation	26
Risk Factors and Signs of Elder Financial Exploitation	30

Chapter	Page
History	32
Current Interventions	35
Internet Crime Complaint Center	36
Caregiver Interventions	36
Money Management	37
Financial Institutions	38
Elder Fraud Hotline	38
Current Issues	40
Where Does Elder Abuse Fit	45
III. Recent Examples of Elder Financial Exploitation in Scam Related Activities	46
IV. Findings and Conclusions	53
V. Recommendations and Implications	55
References	57
Bibliography	63

List of Tables

Table	Page
1. Variations in Definitions of Elder or Vulnerable Adult.....	42

Chapter I: Introduction

Operationalization of terms

For the purpose of this research and review, the term “the elderly” or “elder population” refers to any older adult who is over 60 years of age. This term is outlined from the United States Department of Justice (DOJ) who indicates that an elder is any individual who is 60 years of age or older. (US DOJ)

Introduction

Elder Financial exploitation is one of the most prevalent crimes in modern America, with financial scams at the top of the list of most damaging to the elderly population. While widely unreported, scam related activities targeting elder individuals are rampant. The Consumer Financial Protection Bureau (CFPB, 2017) estimates that the average loss of an elder American who suffered from Elder Financial Exploitation is approximately \$34,200. The CFPB also estimates that there was more than \$6 billion dollars in attempted and actual losses between 2013 and 2017. However, with the rise of telemarketing scams, phishing emails, and other related scams, this number is rising dramatically every year. An outside analysis as ordered by the CFPB estimates that the actual reporting on elder financial abuse and exploitation is nothing more than a drop in the bucket compared to the estimated \$2.9 billion to \$36.5 billion dollars in losses every year (National Council on Aging [NCOA], 2021). While there is a great disparity between those two numbers, it is easy to see that elder financial exploitation has a gigantic impact.

While current law-making bodies and law enforcement agencies are doing what they can to assist in the fight against elder financial exploitation they are limited in the resources on how to stop scam related activities. Yearly monetary losses by the elderly are increasing, state and

federal funding to assist vulnerable adults has not slowed these rates, and funding for the elderly for victim services as well as financial institutions do precious little to protect elders who have fallen victim to a scam.

About the Author

There are many aspects that go into understanding elder financial exploitation, one of the best ways to obtain a full comprehension of these types of cases is actually working them. I have spent over seven years working in the financial industry as a financial crimes investigator working cases related to elder financial abuse, terrorist financing, sex trafficking, and money laundering. In my professional experience I have worked many cases surrounding elder financial exploitation specifically, cases that are related to scam related activities. Additionally, I have worked with many different law enforcement agencies from Secret Service, Department of Homeland Security, Federal Bureau of Investigation, Adult Protective Services, as well as multiple state and local agencies.

In the process of working elder financial exploitation cases I have come to understand that there are many small details that go into understanding the depth of cases related to elder financial exploitation. It is my hope that I can share some of this knowledge with the readers in an attempt to deter and reduce elder victimization in scam related activities.

Background and Need

Public health and welfare officials began to worry about the elder population in terms of financial exploitation in the 1970s, which led to the ratification of the Social Security Act of 1974. Prior legislation related to the Older American's Act will be mentioned later in this reading. The Social Security Act would provide services as well as legal services such as

guardianship to America's aging population. While this was a great first step, prior to the 1990s, elder financial abuse generally had not been considered a crime, it would not be until 2002 that the U.S. Department of Justice accepted elder financial abuse as a criminal justice matter. In 2010, the Elder Justice Act was passed to authorize the expenditure of federal funds that are needed to introduce the law and extend benefits to elders on the federal level, not just on a state level.

Up to 2014, the Elder Justice Act was authorized to spend close to \$770 million, of which two-thirds was earmarked specifically for Adult Protective Services. One of the essential main factors of the Elder Justice Act was that it called for the establishment of forensic centers to support efforts made by legal, medical, social service, and law enforcement agencies to aid in the prevention and prosecution of all types of crimes that are committed against the elderly.

While these interventions have assisted with the growing problem that is elder financial exploitation, it has not ended the ongoing issue. The Elder Justice Act had the intention to assist with elder financial exploitation, it typically does not cover an elder or assist an elder when they are the victim of any type of scam. Speaking from this author's own experience of dealing with elder financial exploitation cases—APS agencies will not pursue a reported elder financial exploitation case unless the perpetrator of the case is known to the victim. From this author's own knowledge from working in criminal financial investigations, elders who fall for a scam, there is little assistance that is provided to them.

Purpose of the Study

The main objective of this thesis is to investigate the current literature and data that has been published in order to better understand elder financial exploitation as it pertains to scam

related activities and the economic implications of these types of crimes and activities. This thesis will be an integrative review and will focus on information that is collected from current published studies as well as statistical information that has been compiled and provided by federal data and from elder financial exploitation reporting bureaus and agencies.

This thesis will also focus on the current variables that surround the issue that is elder financial exploitation related to scam activities including current legislation, criminal justice issues, and reporting issues that go hand in hand with financial crimes that are committed against the elderly.

Research Questions

Current research, as well as the author's knowledge indicates that despite the efforts of law-making bodies as well as federal and state law enforcement agencies to criminalize and deter elder financial exploitation related crimes there continues to be a rise in elder related financial crimes, specifically related to scam activities and fraud from parties unknown to the elder individual. What are the current scams that are affecting the elderly? How are these scams being carried out? How much do elders lose financially as a result of these activities? What are the current interventions have been enacted in order to assist with the deterrence of these activities? What more can be done in order to deter victimization?

This integrative review will explore what scams are currently taking place against the elderly, what the profits and gains are from committing scam related activities, as well as how the United States has created laws and legislation to assist with the protections of elder individuals.

Methods

Setting

Due to the nature of this integrative research review which is primarily focusing on the research and collection of information surrounding issues related to elder financial exploitation in scam related activities, the information within this work was primarily collected via Internet resources, and databases. As well as Internet publications and from the author's own knowledge of having worked elder financial exploitation cases in the financial industry. Further information related to case examples of elder financial exploitation were retrieved from the United States Department of Justice website as well as cases taken from local news stations.

Additionally, information was collected from online databases, government resources, as well as private sector databases in order to obtain a better understanding of the actual scope of victimization, losses, and how scam related activities relate to elder financial exploitation. Furthermore, information was collected from peer-reviewed scholarly publication related to the topic.

One of the most difficult tasks with collecting and compiling the research related to this topic was how drastically the case numbers and losses changed on a year-to-year basis. In one report, it was estimated that the 2020 elder financial abuse cases in the U.S. have grown by approximately 10%, rising from 7.86 million to 8.68 million (Bischoff, 2022).

While some resources and researchers used data from reported number of cases, and other researchers decided to used data from the estimated number of cases, and therefor would report on the estimated losses based on the estimated case. This disparity in information made for difficulty in grasping the depth of the issue.

Chapter II: Literature Review

Introduction

According to the U.S. Consumer Financial Protection Bureau (CFPB), reports of suspicious activity involving the elderly totaled approximately \$1.7 billion dollars in 2017. In that same year, there were 63,500 reports of suspicious activity involving elderly victims, which was four times as many than there was in 2013. According to the CFPB, an outside analysis of elder fraud losses is estimated to be in the range of \$2.9 billion to \$36.5 billion in any given year (NCOA, 2021).

One of the primary reasons for the gap in the approximation of losses is primarily due to the fact that approximately only 1 in 44 cases of elder financial exploitation or elder financial abuse is reported in any way, according to the National Adult Protective Services Association (NAPSA n.d). Further research indicates that approximately 1 out of 18 cognitively intact, community-dwelling elderly adults are affected by elder financial fraud and scams (Burns et al., 2017).

This literature review will examine the current issues, statistics and crimes related to elder financial exploitation, specifically involving scam related activities and how we can better safeguard our elders (and loved ones) from falling victim to financial exploitation.

What is Elder Financial Exploitation and Abuse

Financial Exploitation and Abuse

In order to understand the basics of elder financial exploitation, we first need to know its parameters and how they are currently defined. There are many forms and variations of elder financial exploitation, it is also commonly referred to as financial mistreatment; exploitation;

fiduciary, economic, or material abuse- which encompasses a wide range of conduct. According to Dessin (2003) abuse can occur from numerous actors including family members, caregivers, neighbors, persons holding a power of attorney, and from unknown sources stating that they are from a certain organization with the intent to defraud, i.e., scam artists, fraudsters, and consumer fraud.

One of the most basic definitions focuses on the misuse of another person's assets. The majority of this review will focus on elder financial exploitation (also known as elder fraud, fraud scams) from sources with the intent to defraud under false pretenses.

Who is an Elder? And What is Elder Financial Exploitation?

According to the United States Department of Justice (DOJ) an Elder refers to a person aged 60 years or older. The U.S. DOJ defines exploitation as a “means of forcing, compelling, or exerting undue influence over a vulnerable adult causing the vulnerable adult to act in a way that is inconsistent with relevant past behavior, or causing the vulnerable adult to perform services for the benefit of another” (2020, March 3, page one, paragraph 2). When it comes to financial exploitation, there are many definitions and many actions that fit under the category of exploitation including the use of deception, intimidation, or undue influence by a person or entity in a position of trust and confidence with an elderly person or a vulnerable adult to obtain or use the property, income, resources, or trust funds of an elderly person or entity other than the elderly person or vulnerable adult. However, elder abuse is defined by state law, and the definitions vary state to state (Hafemeister, 2003). Additionally, included in the definition of elderly financial exploitation as set forth by the DOJ is “obtaining or using an elderly person or a vulnerable adult's property, income, resources, or trust funds without lawful authority, by a

person or entity who knows or clearly should know that the elderly person or the vulnerable adult lacks the capacity to consent to the release or use of his or her property, income, resources, or trust funds” (2020, March 3, p. 13) Carolyn Dessin, J.D., Associate Professor of Law at The University of Akron School of Law stated the following:

It is virtually impossible to generalize the definition of “exploitation” from the various states’ definitions of the term, although there are some common themes in many of the definitions. Thus, in defining abuse, states have considered the act itself, the benefit of another, the lack of consent, the object of the exploitive act, and the relationship of the abuser to the victim. (Dessin, 2003, p. 5)

The Elder Individual as a Victim

There are a variety of reasons that the elderly population is an optimal target for victimization of scam related activities, but there seems to be three main factors: health related effects of aging, financial and retirement trends, as well as demographic trends. In regard to health-related factors, one of the key ingredients of this component is cognitive decline as noted by Deane (2018):

Cognitive decline is a key factor, whether brought on by disease or other changes in the aging brain even without the presence of disease. When cognitive decline begins, financial impairment is often one of the earliest signs for patients, families, and doctors. Physical decline and dependency are also risk factors for elder financial exploitation. (p. 3)

When it comes to the wealth of the elderly, this is displayed in terms of income types. From this author’s knowledge of working cases that involve elder financial exploitation it would

seem that elders are more likely to have some sort of steady income in terms of pensions, retirement incomes, social security incomes as well as other investment types. Furthermore, in terms of demographics, the elder population is rising- according to the National Institute of Health (HHS, 2016), the world's older population continues to grow at an unprecedented rate. Today, 8.5% of people worldwide (617 million) are aged 65 and over. This percentage is projected to jump to nearly 17% of the world's population by 2050 (1.6 billion) (Cire, 2016).

The Introduction of Elder Financial Exploitation

Scam Related Activities

According to the Federal Bureau of Investigation (FBI), elders will lose approximately \$3 billion to fraudsters (fraud perpetrators) annually. (FBI, n.d.) These types of crimes often go unreported and can be difficult to prosecute, so they are often considered a “low-risk” crime. On average, the loss per case in an elder financial exploitation or elder fraud case is \$20,015. This number was calculated from the average reported loss from the Financial Crimes Enforcement Network (FinCEN)—which reported annual losses at approximately \$34,200 per case; the FBI Internet Crimes Complaint Center (IC3), which reported annual losses at \$9,175; as well as from state Adult Protective Services (APS) or law enforcement, which estimates losses to be at approximately \$16,670. These crimes also leave the elderly in a vulnerable position, as they tend to be embarrassed or even too devastated to talk about the outcome of falling victim to these types of crimes. The National Council on Aging (NCOA n.d) recognizes the 10 most popular forms of scams as:

Government Impostor Scams

Government impostors call unsuspecting victims and pretend to be from the Internal Revenue Service (IRS), Social Security Administration, or Medicare. They may say you have unpaid taxes and threaten arrest or deportation if you don't pay up immediately. Or they may say your Social Security or Medicare benefits are in danger of being cut off if you don't provide personal identifying information (that can then be used to commit fraud). Government impersonators often "spoof" the actual phone numbers of the government agency or call from the same zip code (202 for Washington, DC). (NCOA, February 19, 2021)

The U.S. DOJ Elder Justice Initiative also mentions the IRS imposter scam—as it is one of the most prevalent today. These types of scams are particularly damaging to elders- as in the automated message the caller typically indicates that all social security benefits will be disabled if the person who receives the phone call does not return the call or speak with a representative. Typically, these “IRS Agents” will utilize fake information, such as agent ID number and tell victims that they owe money to the IRS and it must be paid via wire transfer or from gift cards. The so-called agents will advise the victims that their identification has been stolen or that their social security number has been used to commit a crime, there is a federal warrant out for their arrest from a state that they do not live in or may have never even visited. (Federal Trade Commission [FTC], 2021)

Considering the prevalence of the government imposter scam it is important to note that real government agencies will not call you asking for your personal information while demanding money and threatening to suspend your social security number. Additionally, government agencies will not call, email, text, or send direct messages to individuals on social

media websites asking for any form of payment. Furthermore, from the perspective of working these types of cases, no one from any government agency will ever call asking for an elder to send money in the form of gift cards, wire transfers, cryptocurrency, or cash payments.

The Grandparent Scam

The grandparent scam is so simple and so devious because it uses one of older adults' most reliable assets, their hearts. Scammers will place a call to an older person and say something along the lines of: "Hi Grandma, do you know who this is?" When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity without having done any background research. Once "in," the fake grandchild will ask for money to solve some unexpected financial problem (overdue rent, car repairs, jail bond) and will beg the grandparent not to tell anyone. Because scammers ask to be paid via gift cards or money transfer, which don't always require identification to collect, the senior may have no way of seeing that money ever again. (NCOA, 2021, page 3)

The perpetrators for these types of scams typically are able to gain access to consumers' personal information by collecting data from social media or even by purchasing the information from thieves who specialize in cybercrime and theft. The scammers are able to spoof the caller ID and make it appear as if the phone number is coming from a trusted source or a phone number that seems similar to the grandchild's (FTC, 2021).

Recently, this author had a friend's grandmother fall for the "your grandchild is in jail" scam, who was even at the store to buy gift cards, when the clerk at the checkout advised that she needed to call family to ensure that it was real, as it did not make sense that gift cards would be

needed to bail someone out of jail. Thankfully, the grandmother called my friends mother, who said that she could call her granddaughter to ensure that she was safe, and not under arrest.

Medicare/Health Insurance Scams

Every U.S. citizen or permanent resident over age 65 qualifies for Medicare, so there is rarely any need for a scam artist to research what private health insurance company older people have in order to scam them out of some money. In these types of scams, perpetrators may pose as a Medicare representative to get older people to give them their personal information, or they will provide bogus services for elderly people at makeshift mobile clinics, then bill Medicare and pocket the money. Medicare scams often follow the latest trends in medical research, such as genetic testing fraud and COVID-19 vaccines.

(NCOA, 2021, page 4)

One of the first important factors to note when it comes to Medicare/health insurance scams is that Medicare will never call someone. Most government agencies, if they need to communicate with someone, the first thing that they will do is send a letter. The callers of the scams will represent information to the potential victim that new Medicare, Social Security, or supplemental insurance benefits are being issued and the potential victims file must be updated to receive these bogus benefits. Typically, from the perspective of the author and having worked these types of cases, the scam is carried out by the caller who is able to obtain personal banking information from the victim, which is then used to carry out theft. Unfortunately for the victim, the perpetrators of Medicare scams can get extremely aggressive, calling a potential victim over and over and harassing them at all hours of the day until they comply with the directives of the perpetrator.

Computer Tech Support Scams

Computer technical support scams prey on people's lack of knowledge about computers and cybersecurity. A pop-up message or blank screen usually appears on a computer or phone, telling you that your device is compromised and needs fixing. When you call the support number for help, the scammer may either request remote access to your computer and/or that you pay a fee to have it repaired. The Federal Trade Commission (FTC) found that seniors who fell for this scam lost an average of \$500 each to computer tech support scams in 2018. (NCOA, 2021, page 4)

These types of scams are particularly devastating to the elderly population as the tech scammers ensure that they target and prey on those who know little about computers and technology. The tech support scam wants victims to believe that there is a virus of some kind on their computer, or another sort of serious problem. This is done so that the perpetrator can gain access to the victim's computer via remote access in which a "diagnostic test" is completed. From the author's understanding of how these scams are carried out- the scammer then will take advantage of the lack of knowledge and charge for "services rendered" by asking for payment to be sent via gift card purchases, cash cards, money transfer applications, or wire transactions, all this is done for a problem that did not even exist in the first place.

In some instances, from the author's prior experience, the perpetrator will gain remote access to the victim's computer and place malware software on the computer that is able to recognize key-strokes. In doing so, the perpetrator will wait for the victim to access their banking information, or direct them on how to send them payments in an attempt to take over the victim's account.

Sweepstakes & Lottery Scams

This simple scam is one that many are familiar with, and it capitalizes on the notion that “there’s no such thing as a free lunch.” Here, scammers inform their mark that they have won a lottery or sweepstakes of some kind and need to make some sort of payment to unlock the supposed prize. Often, seniors will be sent a check that they can deposit in their bank account, knowing that while it shows up in their account immediately, it will take a few days before the (fake) check is rejected. During that time, the criminals will quickly collect money for supposed fees or taxes on the prize, which they pocket while the victim has the “prize money” removed from his or her account as soon as the check bounces. Unlike some of the other scams noted here, lottery and sweepstakes scammers can sometimes collect thousands of dollars from their unsuspecting victims. (NCOA, 2021 page 4.)

For sweepstakes and lottery scams the initial contact with the victim typically consists of a phone call, email, notification via social media, or even a letter indicating to the potential victim that they are the winner of a “prize.” These types of scams are usually the epitome of if something is too good to be true it probably is, reason for that being is that the scam perpetrator will typically ask the victim to send the perpetrator money, which is “taxes and processing fees” before the prize money can be sent to the victim. From the experience of the author, much like other types of scams, the perpetrators will ask for the money to be sent via wire transfer, gift card purchases, or cash transaction applications.

In order to keep the payments going, the author has noticed in prior cases the perpetrators often state that the prize is only one more payment away, and will threaten those who want to cut

communication with harm to either the victim or their loved ones. Some will even attempt to report the victim to the authorities.

Robocalls/Phone Scams

In recent years, these types of phone calls are a daily occurrence, and have become a serious nuisance to most. Robocalls take advantage of sophisticated phone technology to dial large numbers of households from anywhere in the world. Robocallers use a variety of tactics to cheat their victims. Some may claim that a warranty is expiring on their car/electronic product and payment is needed to renew it. One popular robocall is the “Can you hear me?” call, where when the senior says yes, the scammer hangs up after recording their voice, thus obtaining a voice signature to authorize unwanted charges on items like stolen credit cards. (NCOA, 2021 page 5)

According to the Federal Communications Commission (FCC), robocalls accounted for over 200,000 complaints each year, which represents about 60% of their total complaint volume (Boyd, 2020). Even more staggering is that 48 billion robocalls were placed in 2018 just in the United States (Balar, 2019).

Robocalls typically consisted of the same tactics such as: claims that the potential victims debit card information has been sold illegally, or been a victim of identity theft, or that there has been suspicious activity on your bank account, or that your Amazon account has been used to make a purchase. Robocalls are often used in IRS scams, vehicle warranty scams, and sometimes even tech support scams (Boyd, 2020).

Romance Scams

As more people use the Internet for dating, con artists see an opportunity to find their next victim. Romance scammers create elaborate fake profiles, often on social media, and exploit seniors' loneliness for money. In some cases, romance scammers may (or pretend to) be overseas, and request money to pay for visas, medical emergencies, and travel expenses to come visit the U.S. Because they drag on for a long time, romance scammers can get a lot of money from a senior—the FTC found that in 2019 alone, seniors lost nearly \$84 million to romance scams. In 2020, that number shot up to \$139 million according to the FTC. Romance scams reached a record high in 2021, increasing by nearly 80% from 2020, according to a report from the Federal Trade Commission. In the past five years, victims have lost more than \$1.3 billion to such scams, the FTC said, more than any other category of fraud the agency tracks. (NCOA, 2021 page 5)

Romance scams are carried out by the victim meeting the perpetrator on some type of social media or dating website. The perpetrator typically moves fast in order to gain the affections of the victim. Most of the stories are incredibly similar—they are out working overseas, they are in the military, they are a doctor of some type working for an overseas outreach program. Sometimes, the perpetrator will disguise themselves as an heir or heiress of a vast fortune and need money in order to “release their funds.” These types of scams also vary in longevity, from the author’s experience, sometimes the perpetrator will take the money and run, and sometimes they will stick with the scam for as long as possible and drain the victim of all their funds.

Romance scams are among the saddest types of scams out there. When this author was working as a security representative at a financial institution it was one of the most prevalent

cases that usually equated to the biggest losses. Not only do you need to explain to the victim that they have fallen for a scam, but you need to also inform someone that the person who said that they love them, and that they want to be with them for the rest of their lives is lying. For most people (mainly single or widowed women) that can be a tough reality, and unfortunately, there are some who will not believe what they are being told.

Internet and Email Fraud

While using the Internet is a great skill at any age, the slower speed of adoption among some older people makes them easier targets for automated Internet scams that are ubiquitous on the web and email programs. Pop-up browser windows simulating virus-scanning software will fool victims into either downloading a fake anti-virus program (at a substantial cost) or an actual virus that will open up whatever information is on the user's computer to scammers. Their unfamiliarity with the less visible aspects of browsing the web (firewalls and built-in virus protection, for example) make seniors especially susceptible to such traps.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, or an online store. Phishing emails request your personal information, such as a log-in or Social Security number to verify your account, or ask that you update your credit card payment. Then they use that information to steal your personal and financial information. (NCOA, 2021 page 6)

Charity Scams

Charity scams rely on seniors' goodwill to pocket money they claim they're raising for a good cause. Some scammers may use a name similar to a legitimate charity. They often capitalize on current events, such as natural disasters, and may set up a fundraising page on a crowdsourcing site, which don't always have the means to investigate fraud. Charity scammers may insist you donate immediately, sometimes with a payment method that should be a red flag—e.g., gift cards or money transfer. (NCOA, 2021 page 6)

The FBI also recognizes in the 2020 *Elder Fraud report* that:

Due to the pandemic, many elderly victims started shopping online for the first time ever.

Elderly victims filled over 14,000 Non-payment/Non-delivery complaints experiencing losses of over \$40 million in 2020, making non-delivery of products the second most reported fraud among the elderly. (DOJ, 2020, March)

Prevalence of Scam Related Activity and Financial Exploitation in Elderly Victims

Prevalence of Elder Financial Abuse

It is hard to get a true grasp on the actual numbers surrounding elder financial abuse, as there are many different sources within the United States that publish very different estimates. In a study by the New York State Office of Children and Family services, it is stated that only 1 out of nearly 24 elder abuse cases were actually reported to the authorities (Huang & Lawitz, 2016). According to the National Adult Protective Services Association (NAPSA), only 1 in 44 cases of financial abuse is ever reported (NAPSA, n.d.).

In a meta-analysis by Yon et al. (2017), the prevalence estimates of elder abuse reported in 52 publications published between 2002 and 2015: the global prevalence of elder abuse (all

types) was 15.7%, or about one in six older adults. Given the approximate 2015 population estimates of 901 million people aged 60 years and older, this rate amounts to 141 million victims of elder abuse (all types) annually on a global prevalence. Of these, it is estimated that approximately 7% of elder adults experience some type of financial abuse or exploitation. (Yon, 2017)

Prevalence of Scam Related Activities

From the author's experience of working in financial crimes, major companies have been victimized in recent years with various cyber-attacks such as ransomware and data breaches that expose the personal information of billions of customers. It would appear that fraud perpetrators are now using this information to disguise themselves as trusted corporations or law enforcement agencies in an attempt to steal financial information and funds from people all over the United States. According to scam protection agency First Orion, over 40% of all calls made in the United States in 2019 were scam calls. In a study of over 5,000 mobile phone subscribers found that 28% of scammers already had their target's information, such as their name, phone number, and address (First Orion, 2019). As a result of this activity, this author, as well as many other individuals known to the author have stopped answering their phones unless the number is recognized to them or similar to phone numbers of people that they may know. To combat this issue, in the author's experience, scammers and fraudsters now use a process called "spoofing," to hide the true phone number that they are calling from to make the phone number look like a legitimate business or person.

Additionally, according to a data release from the Federal Trade Commission (FTC), in 2020 there were more than 2.1 million fraud reports from consumers—with imposter scams being

one of the most common types of reported fraud. Of the top five categories included internet services; prizes, sweepstakes, and lotteries; as well as telephone and mobile services rounded out the top five fraud categories. Additionally, consumers reported losing more than \$3.3 billion to fraud in 2020, which was almost double to what it was in 2019. In 2020, those over the age of 60 accounted for 30% (\$602 million) of the total fraud loss that was reported to the FTC. (FTC, 2021) While this information does in fact indicate that a majority of the losses from fraud related activities were individuals under the age of 60, it is no less alarming.

Prevalence of Scam and Fraud Related Elder Financial Exploitation

The 2010 US Census recorded 40.3 million people aged 65 years or older accounting for approximately 13% of the total population. By the year 2050, it is estimated that elderly Americans are projected to account for 25% of the population. From the perspective of the author, and in order to maintain a grasp on these crimes, a major issue in estimating and recording the true data related to the prevalence of elder financial exploitation is that there is no national reporting system to report the data. While there are many systems that accept the reporting of fraud and financial scams among all citizens, not just the elderly (i.e., FBI, FTC, APS, CFPB, to name a few) from the author's knowledge, there is no national mandatory reporting of elder financial exploitation. Since many states have different laws and definitions related to elder financial exploitation and abuse, and the difficulty in recognizing these types of cases many of the cases go unreported (Hafemeister, 2003).

Each year, millions of Americans will fall victim to some type of financial fraud, exploitation, or internet scheme. The Internet Crimes Complaint Center (IC3) received a total of 791,790 complaints in the year 2020 with losses reported over \$4.1 billion. Based on the

information that was provided within the complaints, approximately 28% of the total fraud losses were sustained by victims who were over the age of 60, resulting in the reported loss of approximately \$1 billion to seniors. This represents an increase of approximately \$300 million in losses reported in 2020 versus what was reported in the prior annual report of victims over the age of 60 in 2019. (IC3, n.d)

In the 2020 IC3 report, the top 10 types of crime by number of victims over the age of 60 is as follows: (It is imperative to note that 9 out of 10 of the top ten methods of loss were some type of fraud or scam related activity.)

- Extortion: 23,100
- Non-payment/non-delivery: 14,534
- Tech support: 9,429
- Identity theft: 7,581
- Phishing/vishing/smishing/pharming: 7,353
- Spoofing: 7,279
- Confidence/romance fraud: 6,817
- Personal data breach: 6,121)
- Misrepresentation: 4,735
- Government impersonation: 4,159

The reported losses from the top ten types of crime are as follows (in no particular order):

- Extortion: \$18,503,168
- Non-payment/non-delivery: \$40,377,167
- Tech support: \$116,415,126

- Identity Theft: \$39,006,465
- Phishing/vishing/smishing/pharming: \$18,829,999
- Spoofing: \$40,886,040
- Confidence Romance: \$281,134,006
- Personal data breach: \$24,641,539
- Misrepresentation: \$1,815,552
- Government Impersonation: \$45,909,970

Utilizing data from state APS, FinCEN, and IC3, Comparitech estimated that the top five states with the highest rate of elder fraud were:

- Oklahoma: 26,661 cases per 100,000 seniors. Reported estimated data approximates 234,00 senior victims with losses at \$4.17 billion.
- Vermont: 39,379 cases per 100,000 seniors. Estimated losses totaled \$676 million per year.

The state of Vermont's APS opened investigations into just 17.5% of reports, and 29% of these related to exploitation. Investigations in the state decreased from 2019 to 2020 by 19%, despite the number of reports from 2019 to 2020 only decreasing by 11%. Citing the pressures of COVID-19 and the fact that the current statute does not address financial exploitation, the number of reports is likely highly underreported/investigated (Bischoff, 2020).

- Alaska: 22,104 cases per 100,000 seniors. Reported estimated data approximates a 39% increase in victims from 2019, with losses in 2020 at \$275 million.
- Delaware: 22,078 cases per 100,000 seniors, with approximate losses at \$386 million.
- Nevada: 21,248 cases per 100,000 seniors, with estimated losses at \$1.34 billion.

When it comes to the estimated losses per state, Comparitech estimates for total elder fraud losses. The top five are as follows:

- California: \$10.8 billion per year
- Florida: \$9.4 billion per year
- Texas: \$8.1 billion per year
- New York: \$7 billion per year
- Virginia: \$5.1 billion per year

In a study conducted by Acierno et al. (2009), titled “National Elder Mistreatment Study,” the researchers found that 6.5% of respondents of a total population group of 5,777 surveyed indicated that they had experienced financial exploitation by a stranger in their lifetime; of the 6.5%, 2.9% indicated that they had their money spent without their knowledge, consent, or authorization; 3.8% had documentation in which their signature had been forged, and 1.4% had been forced to sign documentation that authorized the utilization of funds. (Acierno, 2009).

In 2014, Holtfreter et al. found from survey research in their study titled “*Financial Exploitation of the Elderly in a Consumer Context*,” that in a study of 2000 residents over the age of 60 from the state of Florida and Arizona nearly six out of every ten participants were targeted by a fraud attempt in the year 2010. Approximately 14% of the full sample were a victim of fraud within the past year. The prevalence of victimization was greater among target adults (25%). The most common form of shopping/purchasing fraud attempt was in an attempt to sell a phony magazine subscription or something else. The most common type of financial fraud in the year prior to the study was having someone attempt to trick an individual into providing personal financial information (16%). Financial fraud victimization of any type was rare (.8%). The most

common types of other consumer fraud targeting involved phony prize scams (24%) and contributing to phony charities (22%) (Holtfreter et al., 2014).

In the same study, the authors found that shopping/purchasing fraud and financial fraud cases were rarely made known to law enforcement officials. The study did conclude that when individuals had someone attempt to steal their personal information, 25% would get into contact with law enforcement and report the suspicious attempt (Holtfreter et al., 2014).

Risk Factors and Signs of Elder Financial Exploitation

Financial exploitation from scam related activities can take many forms, from soliciting for fake charities (indicative of money mule activity, or terrorist financing), to telemarketing scams, love scams, and identity theft. Scammers tend to target older adults because they believe that they have a significant amount of money in savings, in addition to consistent income from pensions, 401(k)s, and Social Security benefits. Criminals will often gain their targets' trust or use tactics of intimidation and threats to take advantage of their victims. "Once they are successful, scammers are likely to keep the same scam or scheme going because of the prospect of financial gain," according to Calvin Shivers, assistant director of the FBI's criminal division. There is no easy way to tell when an elder is being victimized, especially when it comes from a financial standpoint. From the author's experience, however, there are a few warning signs and indicators that can be detected in the hopes to catch the exploitation and attempt to stop it in its tracks. A few of these signs are compromised physical wellness, diminished independence, monetary loss (unexpected changes in account balances or banking practices), financial dependence, psychological declines, loneliness, depression, anxiety and sleep disorders. Regarding scam related activities, the author has noticed that warning signs may include a

sudden transfer of funds via international or domestic wire transfer or automated clearing house (ACH) transfer to an unknown individual, purchase of gift cards or money orders, checks made payable to unknown individuals, or even unidentified debit card purchases made outside of the elderly individuals known geographic location.

One of the major steps in combating elder financial exploitation is recognizing the risk factors that increase victimization. In a study conducted by Acierno et al. (2010) the researchers found that:

Considering lifetime stranger-perpetrated financial mistreatment, statistically significant risk factors included age below 70, minority racial status, poor health status, prior experience of a traumatic event, low social support, and required assistance with daily activities. Multivariate analyses showed that only lower age, poor health, prior traumatic events, and needed assistance with activities of daily living uniquely contributed to risk of stranger-perpetrated financial exploitation. Thus, a greater number of risk factors predicted stranger, vs. family-perpetrated financial mistreatment.

It is important to understand that every case is as different and unique as the elder that has been victimized, and things are not always black and white. There have been numerous studies that have offered insight as to why certain elderly people are more susceptible to and targeted for financial exploitation.

In the prior mentioned study by Holtfreter et al. (2014), the researchers found that scam targeting of elderly individuals is least common among those who are eighty years of age or older, their research indicating that less than half (49.6%) of the surveyed individuals indicated that they have been targeted. Which in contrast over 60% of the other respondents over the age

of 60 indicated that they have been targeted. Males had been reported to be targeted more frequently than females (65.4% compared to 56.4%, respectively). Education levels were not significantly associated with victimization and targeting. When it came to racial and ethnic minorities, there were no differences observed when it came to being the target of scam and fraud activities- however, racial minorities and those who were retired were more likely to report that they had been the victim of fraud (Holffreter et al., 2014).

When a further look is taken into the abuser profile there appears to be research regarding elder financial exploitation, however the abuser profile related to those who commit scam activity is relatively lacking. In a study conducted by DeLiema et al. (2018) researchers noted that:

Abusers fall into 4 profiles descriptively labeled "Caregiver," "Temperamental," "Dependent Caregiver," and "Dangerous." Dangerous abusers have the highest levels of aggression, financial dependency, substance abuse, and irresponsibility. Caregivers are lowest in harmful characteristics and highest in providing emotional and instrumental support to victims. The 4 profiles significantly differ in the average age and gender of the abuser, the relationship to victims, and types of mistreatments committed. (p. 1)

History

According to the U.S. DOJ, elderly financial exploitation is one of the most frequently reported forms of elder abuse, despite the fact that a majority of the cases go unreported. Elder mistreatment—neglect, financial exploitation, physical, psychological, and sexual abuse—is a growing problem in aging societies, yet there is little consensus on what interventions best serve the needs of victims and society (Moore & Browne, 2016).

The Advent and Rise of Protective Services

Public welfare officials were faced with an increasing number of older persons who were unable to manage on their own and began to develop a new approach to providing services, which they called “protective services units.” It was an approach that would provide not only social services, but also legal assistance, particularly guardianship (Hafemeister, 2003).

As such, the Older American’s Act (OAA) was enacted in 1965. This act supported a large range of home and community-based services, such as meals on wheels, in home services, legal services, elder abuse prevention, and caregivers’ support. These programs assisted elders with staying as independent as possible in their own homes and communities (National Committee to Preserve Social Security & Medicare [NCPSSM], 2021).

As a part of the Social Security Act of 1974, congress passed legislation that provided funds to states to assist in the development and implementation of protective services. Initially, it appeared that the projects were costly, and effectiveness was questioned after studies were published that displayed the questionable outcomes, and partially it appeared to infringe on the rights of elders. After much back and forth, and case studies within congress, Surgeon General Louis Sullivan (Wolf, 2003) declared in the 1980s that elder abuse and neglect was a public health and criminal justice issue- leading to a rise of the criminalization of elder abuse. While estimates of the prevalence of the problem continued to rise, accurate data collection of actual cases served by local Adult Protective Services programs continued to be difficult to achieve due to a lack of uniform definitions and reporting requirements (Otto, 2000).

By 1991, 42 states had mandatory reporting laws, in which certain crimes and instances need to be reported to Adult Protective Services (APS), and 34 states were providing protective

services to the impaired and elderly. Mandatory reporting had become constantly debated issue which was seen by some as a threat to client autonomy (NAPSA, n.d.). A study in 1991 by the Government Accounting Office concluded that mandatory reporting did not necessarily prevent abuse. The study identified a number of other factors that were more effective in abuse prevention. The study also pointed out that mandatory reporting was second only to public and professional awareness in effectiveness in case identification (NAPSA, n.d.). By the end of the 1990s, there were only five states that did not have some type of mandatory reporting system.

Prior to the 1990s, elder financial abuse had generally not been considered a crime (Krienert et al., 2009). However, Pillemer et al. (2016) shifted the conceptualization of elder abuse and challenged prior assumptions in the caregiver stress model. Their research revealed that elder abuse differed in many ways from the prior accepted models that it was closely related to child abuse in how it is carried out, thusly shifting the focus from the victim's role in elder abuse to that of the abuser (Jackson, 2015). The impact of this research in reshaping the field of elder abuse cannot be understated. In 2002, the U.S. DOJ became involved in elder abuse through the Department's Nursing Home Initiative of Justice for elder abuse research and assisted with funding to the National Institute of Justice for elder abuse research. As a result of this, elder abuse was an accepted phrase in the Department of Justice and became a matter of criminal justice. Falk et al. (2012) noted that:

At that juncture, the notion of elder justice, as opposed to elder abuse or elder mistreatment, served as a vehicle to communicate a message that would speak to the broader human rights issue of freedom from abuse and exploitation. That same year, the Elder Justice Coalition was formed, bringing together advocates committed to the reform

of social policy for the protection of elders. From 2003 forward, the coalition fought to ensure that the Elder Justice Act would be signed into law. (Falk et al., 2012, page 2, paragraph 5)

From the author's experience, social programs that are federally funded are not without their limitations. Unfortunately for a number of elders, APS will only take on cases in which the perpetrator is known to the victim. In the instance of elder financial exploitation of scam and fraud related activities- there is not much these programs can do to help them. Occasionally, an APS worker can take the time to go out and check on the elder in the event of financial exploitation and falling for some type of scam, but it is not a general rule and is not mandatory for APS agents.

Current Interventions

Currently in the United States there are multiple government interventions that assist elders and attempt to reduce fraud and exploitation. Most of these interventions are still fairly new—however from the knowledge of the author in working elder financial crime cases, interventions from caregivers, financial institutions, as well as money managers have been the primary defense in the prevention of elder financial exploitation.

Elder Justice Act

Although the act was first introduced in the early 2000s, the Elder Justice Act (EJA) was passed in 2010. One of the primary provisions of the Elder Justice Act was to authorize the expenditure of federal funds needed to implement the law and provide benefits to elders on a national level, not just on a state level and based off of states budgets (EJA, 2010). In the years of 2010 through 2014, the EJA authorized close to \$770 million in spending, in which \$500

million was specifically earmarked for Adult Protective Services (NAPSA). Even though the EJA operates on a federal level, the main operation of the act is specifically for providing funding, and elder justice will continue to be addressed in the criminal arena at a state and local level and under state and local jurisdictions (Falk et al., 2012). Part I of the Elder Justice act calls for the formation of the Elder Justice Coordinating Council, which is comprised of federal government representatives charged with the responsibility of administering programs for the promotion of elder justice (Falk et al., 2012). This council in turn provides recommendations to the Secretary of the Department of Health and Human services on issues that are related to abuse, neglect and exploitation of the elderly. Another key provision of the EJA is that it calls for the establishment of forensic centers to support collaborative efforts made by legal, medical, social service, and law enforcement agencies for the prevention and prosecution of crimes against the elderly (Legal Information Institute, Public Law 111-148, 2010).

Internet Crime Complaint Center

The FBI, in alignment with the Department of Justice Elder Fraud Initiative created an avenue to report fraud through the IC3. Which receives and tracks thousands of complaints daily, which are reported by victims of fraud. According to Calvin Shivers, assistant director of the Criminal Investigative Division of the FBI:

This reporting is key to identifying, investigating, and holding those accountable for their actions. Victims of fraud have the option to identify their age when submitting a complaint to the IC3; the information in the IC3 report is derived from complaints submitted by or on behalf of victims aged 60 and over. (DOJ, 2020, March).

Caregiver Interventions

The role of caregiver and family members have been among the first models to be used in preventing elderly abuse of all kinds. These types of interventions include education, support groups, and community-based activities in order to ensure that elders are more educated about the dangers of financial exploitation and fraud activities. More importantly, however, is the role of adult family members or friends who are able to assist an elder with their finances. One of the most important aspects of preventing elderly financial exploitation is ensuring responsibility while maintaining autonomy. It is imperative that a caregiver is aware of where the elder is spending their funds and ensuring that they are educated in terms of current scam related activities, especially phishing and government imposter type scams. This is outlined by Holtfreter et al. (2014):

“The fact that few fraud attempts or actual fraud victimization events are reported to law enforcement suggests the need for education about the importance of reporting such events and, at the same time, for efforts to ensure that law enforcement respond to such reports in a proactive and well-publicized manner. Such steps can increase the chances that the elderly will learn about consumer fraud victimization, that they will report it, and that a potential general deterrent effect can be created or increased. For example, would-be offenders, such as family members and solicitors, may be less likely to engage in fraud if they read or hear about law enforcement aggressively responding to claims of fraudulent activity.” (p. 19)

Money Management

One of the biggest issues in elder financial exploitation is money management, and the accumulation of wealth—and unfortunately sometimes, we see the opposite: poverty. This is

especially prevalent in cases in which the spouse or partner who was managing the finances passes away without establishing wills, trusts, and executors. When an elderly individual falls victim to a scam, especially a repeat one, it may be difficult for them to fully comprehend the gravity of the exposure if they are not on top of their finances or don't have access to their financial statements. Pillemer et al. (2016) noted that:

Extensive case study reports suggest that individuals vulnerable to financial exploitation can be helped through money management programs. Such programs feature daily money management assistance, including help with paying bills, making bank deposits, negotiating with creditors, and paying home care personnel. These programs are targeted to groups at high risk for financial exploitation and in particular individuals with some degree of cognitive impairment and who are socially isolated. This intervention is also promising, as the preventive potential is high and with well-trained and accredited money managers, the risks of adverse outcomes are low. (Pillemer et al, 2016, Money Management Programs)

Financial Institutions

From the perspective of a financial institution, it is considered mandatory reporting if there is an indication of any type of financial fraud, abuse, or exploitation, and needs to be brought to the attention of APS under state jurisdiction. In most states these cases are also mandated to be reported within a certain timeframe. This however does not come without its limitations: in most cases of fraud or an elder falling for a type of scam related activity, APS can only take on a case in which the perpetrator is known to the victim. In the instance of an elder becoming the victim in a fraud/scam scenario, APS may take the time to go check in on the

elder, but other than that there is not much that can be done. From the author's prior experience, given the prevalence of scam related activities, prosecution of these cases are few and far between.

Elder Fraud Hotline

United States Attorney Aaron L. Weisman (2020) stated that,

“This office has zero tolerance for those scammers who would target our senior or other vulnerable citizens for financial exploitation. As demonstrated by this Office's zealous prosecution of such scammers, defrauding our seniors of their hard earned savings is a sure way to being subject to federal prosecution and, if convicted, incarceration.”

Which leads to the March 3, 2020 report by the United States DOJ, Attorney General Barr who announced the launch of a National Elder Fraud Hotline, which provides services to seniors who may be victims of financial fraud. The Hotline is to be staffed by experienced case managers who can provide personalized support to callers. Case managers will assist callers with reporting the suspected fraud to relevant agencies and by providing resources and referrals to other appropriate services as needed. When applicable, case managers will complete a complaint form with the FBI's Internet Crime Complaint Center (IC3) for Internet-facilitated crimes and submit a consumer complaint to the Federal Trade Commission on behalf of the caller (DOJ, 2020, March 3).

Current Issues

Lack of Reporting

A major concern surrounding elder financial exploitation and being able to get a full grasp of how far reaching these crimes are, is that seniors are typically less inclined to report

fraud because they may not know how, feel ashamed that they have been scammed, or in some cases- may not even know that they have fallen victim to a scam. Additionally, elders may feel as if they do advise someone of the fraudulent activity that they have fallen victim to that their family members may lose confidence in their ability to be responsible for their own funds and ability to money manage, therefore losing a sense of independence and sense of self.

Furthermore, it is the experience of the author that when elders do go to report a crime, they may be unable to communicate detailed information to law enforcement, family, or their financial institutions due to cognitive decline, or lack of understanding of how the crime was even perpetrated. They may be under the impression that their computer did have a virus and they needed a tech support representative to help them remove it, and subsequently repay the tech support in gift card. They may have even thought that their vehicle warranty was out, and that they needed someone to call and help them.

In their study, Holtfreter et al. (2014), noted that:

Despite increased concerns about fraudulent activities that target the elderly—evidence in all 50 states having enacted elder abuse statutes in recent decades—little remains known about the prevalence of such fraud, the factors that give rise to it, or the effectiveness of efforts aimed at reducing it. Without information along each of these dimensions, it is difficult to develop and implement evidence-based policies aimed at preventing and reducing elderly fraud victimization. This problem assumes greater importance given the aging of the American population and the increase of elderly populations in upcoming years. (p. 7)

Many Definitions

An additional issue with researching and starting to assist with issues surrounding elder abuse and financial exploitation is that there are endless definitions of elder abuse. Legal definitions of abuse vary by state or federal statute. For example, the Centers for Disease Control and Prevention (n.d) states that “elder abuse is an intentional act or failure to act that causes or creates a risk of harm to an older adult. An older adult is someone age 60 or older. The abuse often occurs at the hands of a caregiver or a person the elder trusts.” The issue with this definition is that the term “older adult,” or “older people” does not fit the definition that is outlined by the United States Department of Justice, in which an elder is someone who is over 60 years of age.

The National Research Council (2003) states that elder abuse is “(a) intentional actions that cause harm or create a serious risk of harm to a vulnerable elder by a caregiver or other person who stands in a trust relationship to the elder, or (b) failure by a caregiver to satisfy the elder’s basic needs or to protect the elder from harm.” (page 17)

Additionally, the World Health Organization (WHO) indicates that “Elder abuse can be defined as "a single, or repeated act, or lack of appropriate action, occurring within any relationship where there is an expectation of trust which causes harm or distress to an older person."(WHO, 2021) Elder abuse can take various forms such as financial, physical, psychological, and sexual. It can also be the result of intentional or unintentional neglect.” In addition to the other definitions that are outline within this research. As such, a lack of consistency in definitions and data elements on elder mistreatment across jurisdictions makes it challenging for researchers to measure elder mistreatment and identify trends (Carney, 2019).

While the U.S. government has passed several laws to protect elders, one of the true

issues arises when it comes to the differences in statutes by state. This issue, it seems, can be broken down into two main categories: who is classified as an elder, and what constitutes exploitation.

For example, in California and Florida, an elder is anyone who is 65 years of age or older. In Illinois, New York, and Massachusetts an elder is 60 years of age or older. Arizona does not have specific elder abuse legislation and uses the term “vulnerable adult.” (Hamp, 2003).

In terms of exploitation, state statutes also vary greatly from state to state. For example, in Florida exploitation occurs when a person who: 1) Stands in a position of trust and confidence with a vulnerable adult and knowingly, by deception or intimidation, obtains or uses, or endeavors to obtain or use, a vulnerable adult's funds, assets, or property with the intent to temporarily or permanently deprive a vulnerable adult of the use, benefit, or possession of the funds, assets, or property for the benefit of someone other than the vulnerable adult; or 2) Knows or should know that the vulnerable adult lacks the capacity to consent, and obtains or uses, or endeavors to obtain or use, the vulnerable adult's funds, assets, or property with the intent to temporarily or permanently deprive the vulnerable adult of the use, benefit, or possession of the funds, assets, or property for the benefit of someone other than the vulnerable adult; “Exploitation” may include, but is not limited to: 1) Breaches of fiduciary relationships, such as the misuse of a power of attorney or the abuse of guardianship duties, resulting in the unauthorized appropriation, sale, or transfer of property; 2) Unauthorized taking of personal assets; 3) Misappropriation, misuse, or transfer of moneys belonging to a vulnerable adult from a personal or joint account; or 4) Intentional or negligent failure to effectively use a vulnerable

adult's income and assets for the necessities required for that person's support and maintenance (Hamp, 2003). In Idaho, the definition of exploitation defined as “means an action which may include, but is not limited to, the misuse of a vulnerable adult's funds, property, or resources by another person for profit or advantage” (Hamp, 2003).

As follows is a table of five midwestern states showing the differences in definitions in terms of what defines an elder (if any definition exists), or vulnerable adult.

Table 1

Variation in definitions of elder or vulnerable adult

State	Statute
Minnesota	<p>Subd. 21. Vulnerable adult. (a) “Vulnerable adult” means any person 18 years of age or older who:</p> <p>(1) is a resident or inpatient of a facility;</p> <p>(2) receives services required to be licensed under chapter 245A, except that a person receiving outpatient services for treatment of chemical dependency or mental illness, or one who is served in the Minnesota Sex Offender Program on a court-hold order for commitment, or is committed as a sexual psychopathic personality or as a sexually dangerous person under chapter 253B, is not considered a vulnerable adult unless the person meets the requirements of clause (4);</p> <p>(3) receives services from a home care provider required to be licensed under sections 144A.43 to 144A.482; or from a person or organization that offers, provides, or arranges for personal care assistance services under the medical assistance program as authorized under section 256B.0625, subdivision 19a, 256B.0651, 256B.0653, 256B.0654, 256B.0659, or 256B.85; or</p> <p>(4) regardless of residence or whether any type of service is received, possesses a physical or mental infirmity or other physical, mental, or emotional dysfunction:</p> <p>(i) that impairs the individual's ability to provide adequately for the individual's own care without assistance, including the provision of food, shelter, clothing, health care, or supervision; and</p> <p>(ii) because of the dysfunction or infirmity and the need for care or services, the individual has an impaired ability to protect the individual's self from maltreatment.</p>

Table 1 (continued)

Wisconsin	6.90 Elder abuse reporting system. (br) "Elder adult at risk" means any person age 60 or older who has experienced, is currently experiencing, or is at risk of experiencing abuse, neglect, self-neglect, or financial exploitation. (bt) "Elder-adult-at-risk agency" means the agency designated by the county board of supervisors under sub. (2) to receive, respond to, and investigate reports of abuse, neglect, self-neglect, and financial exploitation under sub. (4).
North Dakota	A vulnerable adult is any person older than age 18, or emancipated by marriage that has a substantial mental or functional impairment.
South Dakota	(3) "Elder," a person sixty-five years of age or older;
Iowa	"Vulnerable elder" is defined in Iowa Code § 235F.1(17) as "a person sixty years of age or older who is unable to protect himself or herself from elder abuse as a result of age or a mental or physical condition."

Penalties of Elder Financial Exploitation

The penalties of elder financial exploitation vary by state to state and are as different as the various definitions of the crime itself. For example in the state of Florida the penalty for elder financial exploitation valued less than \$10,000 is a third-degree felony, which is punishable by up to 5 years in prison and a \$5,000 fine; if the property was valued at \$10,000 or more, but less than \$50,000, is a second-degree felony which is punishable by up to 15 years in prison; if the property is valued at \$50,000 or more, then the crime is a first degree felony and punishable by up to 30 years in prison (DOJ, n.d.).

In the state of Rhode Island, if the property is valued at less than \$500, the personal shall not be imprisoned for more than 5 years, and a fine of not more than \$5,000. If the funds are more than \$500, but less than \$100,000 the person can be subject to not more than 15 years, and a fine of not more than \$10,000. If the property or funds is valued at more than \$100,000, the person can be subject to no more than 30 years in jail and not more than \$15,000 (DOJ, n.d.).

Arkansas has a lower cut-off for max penalty, if the property is valued at \$200 or less, it's a Class A misdemeanor, if the property is valued at more than \$200 or less than \$2,500 the

individual is guilty of a Class C felony; and if it is more than \$2,500 the individual is guilty of a Class B felony (DOJ, n.d.).

Where Does Elder Abuse Fit

Another primary issue when it comes to elder financial exploitation is that there is debate as to where it should be handled, and who should handle it. Because of the nature of these cases, they are widely diverse. There could be a case where an elder is targeted purely due to their age, another case where the elder is targeted because of their access to steady monthly income as well as their cognitive state; or another case because of their health. Recognition of the diversity and range of complexity of elder abuse cases supports the assertion that forms of elder abuse are sometimes a crime, sometimes a medical issue, and sometimes a social services issue, and sometimes a combination of these and more. Consequently, a one-size-fits-all response is unacceptable (Jackson, 2014).

Chapter III: Recent Examples of Elder Financial Exploitation in Scam Related Activities

In the case of, Shawn Whitfield, 49, of Pawtucket, admitted to receiving more than \$109,000 in upfront payments from victims, most of whom were elderly, who were led to believe they had won cash or prizes in a lottery or sweepstakes. Some victims were told they had won as much as \$82 million. Other victims were told they were in line to receive \$5,000 a week for life. Mercedes Benz vehicles were among the valuable prizes some of the victims were told they had won. In each instance, the victims were told their winnings would not be released to them without upfront payment of taxes or fees. The majority of funds collected by Whitfield were transferred electronically to co-conspirators and others, most often to individuals in Jamaica (DOJ, 2019).

In another case, “Mrs. Smith” calls her financial professional requesting the withdrawal of a large amount of money from a brokerage account. Her son calls an hour later to tell the professional that his mother is being scammed into giving money to bail “General Michael Smith” out of jail in Afghanistan. The son says his mother cannot be convinced that she is being scammed and insists on paying the money to ensure the release of the “general” (Lassoff, 2018).

In a case in which the perpetrator was caught, according to the U.S. DOJ two individuals from Houston and three from Atlanta were charged in a U.S. district court for allegedly participating in online romance scams that targeted more than two dozen elderly victims out of more than two million dollars. The scam began in May 2015 where the victims were contacted on online dating sites and through social media feigning romantic interest. The perpetrators would then begin to gain the trust of the victim and were convinced to send them funds.

According to court documents, one of the victims was a 76-year-old widow from Rhode Island who refinanced her home, sold property she owned in Massachusetts, and withdrew funds from bank accounts, over time sending more than \$660,000 to bank accounts allegedly controlled by members of the conspiracy. The woman told investigators she reluctantly made the transfers at the direction of “General Mathew Weyer,” who claimed to be stationed with the U.S. Army in Afghanistan, and whom she met online on Words with Friends (DOJ, 2019). The perpetrators in this case were faced with charges such as committing wire fraud and mail fraud; conspiracy to commit money laundering; mail fraud; and wire fraud.

In another case that is a little closer to home, U.S. attorney Erica H MacDonald announced the guilty plea of Brian J. Williams of Minnesota, to one count of conspiracy to commit mail fraud. The guilty plea came after the indictment of 60 individuals for their involvement in the sale of fraudulent magazine subscription. Williams owned and operated several companies that were involved in the sale of the fraudulent subscriptions including companies called Reader’s Club Home Office, Pacific Renewal Services, and Tropical Readers, located in St. Paul, MN and another located in San Diego, CA. In an apparent phone scam, companies were disguised as telemarketing centers in which telemarketers used deceptive sales scripts that were designed to defraud the victims by tricking them into signing up for expensive magazine subscriptions. In total, Williams and his companies defrauded thousands of victims all over the country out of more than \$29,000,000.00. According to William’s guilty plea, he agreed to pay \$29,262,249 in restitution and faces more than 30 years in prison. This case is the result of an investigation conducted by the United States Postal Inspection Service and the FBI.

Additional assistance was provided by the Treasury Inspector General for Tax Administration (TIGTA) and the Minnesota Attorney General's Office (DOJ, 2020, October 30)

Recently, in St. Louis, MO an 81-year-old woman was the victim of a romance scam, who then opted to help her online boyfriend defraud others. Despite the warnings from many federal agencies the woman decided to keep assisting her "boyfriend," and was arrested and charged. The victim would receive MoneyGram wire transfers from senders that she did not know, and deposited counterfeit and fraudulent checks from remitters in which she had no relation. Additionally, she would allow her "romantic interests to transfer funds through her accounts. In one instance, the victim deposited a check in the amount of \$100,000.00 from another individual who was also a victim of a romance scam. A portion of the funds she kept and sent the rest to her online love interest. In November 2021, she pleaded guilty to a number of federal crimes because of her participation in money mule schemes (Held, 2021).

On November 11, 2021, NBC reported about a Tampa, Florida woman who lost more than \$700,000.00 in an apparent "grandparent" scam. The elder was scammed over the summer when perpetrators were able to convince her that her granddaughter was in legal trouble after being in a car accident and needed her help. The perpetrators told the elderly woman to begin making withdrawals from her bank account and hand the money over to a courier. A man got on the phone with the elder, pretending to be the granddaughter's lawyer, after a woman spoke with the elder who claimed to be her granddaughter. They were able to convince the woman to make withdrawals from different branches at BB&T bank, ending at \$100,000.00 when the elderly victim ran out of funds. When the bank's system alerted staff of the unusual activity, the bank called the victim to inquire as to what she was doing with the funds. The elder advised that she

was using the funds for home improvement and that the contractors wanted to be paid in cash. The Hillsborough County Sheriff's office is asking for the help of Uber, to find the person who stopped at the elder's address posed as a "courier."

The elder's lawyer has filed a lawsuit against Truist Bank (subsidiary of former BB&T) for alleged negligence in their due diligence for allowing the woman to make large and unusual withdrawals even after the red flags were raised. This is despite the fact that the financial institution took the time to reach out to the elderly customer in regard to the suspicious transactions and attempt to verify with her the reasons behind needing the funds as well as the suspicious withdrawals and amounts (NBC Universal News Group, 2021).

Recently, in Falls Church, VA a 78-year-old man fell victim to a romance scam after he had created a social media profile on the dating site called iFlirt. He had made contact with an individual who identified herself as a 30-year-old-widow who feigned interest as a potential love interest. As the relationship grew, the scam started to show itself as the woman claimed that she was from New York and was arrested in Germany while attempting to retrieve an inheritance of gold bars and needed the money to make bail. The elderly victim paid for the "bail" only to get arrested a second time and in need of more "bail" money. At the end of the scam, the elderly victim lost over \$500,000 to the fraud.

Two of the individuals who were a part of the scam were Ghanian nationals whose roles in the scam involved money muling activity. The individuals never actually made contact with the victim but they did take part in the laundering of the ill-gotten funds for a profit of 5% to 10% of the proceeds. The prosecutors estimate that the scheme has target multiple victims and

has raked in more than \$42 million, much of which has gone to Ghana, the headquarters of the scam related activity (Barakat, 2022).

In a related scam to Ghana, Richard Dorpe, a Ghanaian national, portrayed himself as a balding 57-year-old white man from Virginia Beach named “Jerry Linus” on the “OurTime” senior dating website. He conned a 68-year-old widow from Chesapeake out of more than \$300,000, as well as items including clothes, a computer and jewelry. When the widow ran out of cash, she took out a home equity loan (Barakat, 2022).

A New Jersey woman has admitted to scamming seniors nationwide out of gigantic sums of money. One of her victims was a 94-year-old woman who she swindled \$500,000.00 from, all by telling the victims that they had won the lottery. The perpetrator was a part of an international group that called and conned seniors out of almost \$700,000. In the scam, the victims would receive phone calls alerting them that they had won prizes and other large sums of money, but they would have to make “pre-payments” in order to receive the funds. The victims, who were promised money and prizes, would then send their checks to the perpetrators. The 94-year-old sent one of the perpetrators 22 checks totaling more than \$500,000 after she had been advised that she won a \$6 million Publisher’s Clearing House sweepstakes.

In the same scam, a 75-year-old female victim who was told that she had won \$2 million and a new car from Kentucky was conned into buying cell phones and gift cards—in addition to the \$30,000 in checks that she sent to one of the perpetrators. An 86-year-old woman from Indiana sent the perpetrators \$20,000 in checks after she had been told that she won a “large sum of money and a car.” FBI arrested one of the perpetrators and charged her with conspiracy to commit wire fraud (DeMarco, 2022).

In a case from Asheville, North Carolina, an elderly man had hundreds of thousands of dollars' worth of cryptocurrency returned after falling victim to a government imposter scam. According to the case, the elder was contacted by scammers who stated that they were with the "Office of the Inspector General," and had the victim convinced into thinking that his money had been used to commit several crimes. One of the scammers identified himself as an agent from the Office of the Inspector General and told the victim that he was required to put the funds into a secure government account until it was verified that the victim himself was not a participant in any of the alleged criminal activity. The victim transferred \$574,766 worth of Bitcoin to a Coinbase account that was being run by the scammers (WLOS, 2022).

In a Medicare scam reported by Kenosha County, Wisconsin there were reports of a new scam targeting the elderly population. The scam itself was set by the scammer introducing themselves as working with Medicare and asking for the last four digits on their "new plastic Medicare card," in an attempt to verify that they received it. According to the report, the scammer was able to confirm the attempted victims address as well as her spouse's name. While attempting to build trust in the victim, the scammer would ensure that they were not going to be asking for their social security number, just wanted to confirm that they had received the card itself. The victim would give the full card number, concerned that they did not have the correct or current card, in doing so they would fall victim to the scam so their Medicare card would be used by someone else (Arndt, 2022).

In Los Angeles, a 77-year-old retired teacher fell victim to a tech support scam when a pop-up appeared on her computer stating that there was an issue that required her attention. In the pop-up it provided the victim with a phone number that she could call in order to get the

problem resolved. The victim called the number that was provided, which initiated a 3-day ordeal that resulted in scammers convincing her that her credit card had been used to spend \$15,000 on child pornography from China. The scammers told her that they could fix the issue, but it would cost her \$45,000 in gift card purchases. She was told that if she did not comply with the wishes of the scammer that they would expose her for taking part in the purchasing of child pornography, there was a warrant for her arrest, and that there were indications that she was taking part in money laundering (Rhode, 2022).

As a result of the ongoing conflict in Russia, scammers are attempting to monetize off people's desire to help Ukraine and establish charity scams via email. There has recently been an escalation of new domain names in order to steal information from potential donors sending money to Ukraine. In a report from Cyren, an email security firm, there has been over 100,000 spam emails per day attempting to get victims to donate to Bitcoin or Ethereum wallets that have been set up by the perpetrators. Their report found that the emails were spoofed by using false Ukraine domains in an attempt to make the emails look authentic. Some of the scammers had even attempted to use Gmail addresses to defraud their victims. Additionally, scam emails were directing the victims to recently created websites that were a front for official charities to benefit the people of Ukraine (Binder, 2022).

Chapter IV: Findings and Conclusions

Elder financial exploitation and abuse could easily be considered the crime of the 21st century, the targets are easy, the gains are typically plentiful, and the costs outweigh the risks due to an extreme lack of reporting and prosecution rates of these cases. As advised earlier within this work, it is the knowledge and understanding of the author the victimization rates as well as the number of fraud attempts are continually on the rise which appears to be giving way to more monetary losses by elders than has ever been seen or reported in the United States.

Given the evidence presented in the currently available literature, a one-size-fits-all conclusion just does not work well for cases that have such a wide range of variables and statistics. As disciplines recognize the multidimensional nature of elder abuse, there is a greater interest in responding with a multidisciplinary approach (Jackson, 2015). However, there are measures that we can take as citizens to help protect elders from harm: such as more education, better implemented programs for elders to receive assistance when they have been victims of scam related activities as well as paying more attention to what elders are spending their money on. One of the key concepts in understanding elder financial exploitation in scam related activities is that there really is no accurate grasp on exactly *how* bad the issue is. Primarily, efforts need to be made in order to educate elders on financial scams and how they can report that they have been victimized by any of the above-mentioned scam related activities.

Studies have recognized that projections of abuse are likely to underestimate the actual population prevalence of victimization. For every incident of abuse reported to authorities, nearly 24 additional cases remain undetected (Pillemer, et al., 2016). Underreporting may be caused by a number of factors, as was previously discussed, these reasons include an older person's fear of

retaliation by the offender, reluctance to disclose the incident because of shame or embarrassment, concern they will be institutionalized, dependency on the offender, and an inability to report because of physical limitations or cognitive impairments (Baker et al., 2016). Most scholarly publications estimate that at least one in ten elders have experienced some type of abuse in any given year- this includes a wide range of different types of abuse, from physical, mental, or financial.

In August 2020, Comparitech, as well as a team of 30 security researchers, writers, and developers compiled and extrapolated data from government reports and registries related to elder fraud in the United States. This company estimated that around five million seniors in the US were subject to elder fraud each year, which resulted in potential losses of close to over \$27 billion (Bischoff, 2020).

According to the National Council on Aging (2021), there are over 200,000 scam and financial abuse cases that are reported to authorities every year, and as stated multiple times throughout this writing, that number is more than likely just scratching the surface. Comparitech estimates that the actual number of cases are estimated to be at over 7.86 million cases every year with over \$148 billion in losses (NCOA, 2021). Regardless of the numbers and statistics, it appears that elder financial exploitation is getting worse every year and current interventions are falling short in offering protection.

Chapter V: Recommendations and Implications

As a financial crimes investigator with over seven years' experience in working in the financial industry, working closely with law enforcement, and working elder financial exploitation cases it is fairly easy to have a broad perspective on the ins- and outs of these case types. This is mainly due to the fact that I am able to have a unique perspective and offer a different type of solutions than someone that comes from a law enforcement perspective or someone that comes from an academic perspective.

It would be incredibly naïve to state that elder financial abuse is preventable aspect, however, given my experience and knowledge regarding the subject there may be a few things could be done in order to reduce the cases of elder financial exploitation in scam related activities. First and foremost, the most important aspect in the potential reduction of cases and victimization is knowledge. Knowledge is always power, and education of the current workings of government entities, computer skills, as well as the current types of scams would be an incredible useful tool in helping to prevent crime. While it is easy to say these types of things will help, the delivery of education is the most difficult aspect, and one delivery method is not necessarily better than another.

Secondly one the most important and probably one of the most effective ways to prevent an elder individual from falling for any type of scam is paying close attention to what the individual is spending their money on. This typically can fall under the category of communication, but also ensuring that a trusted individual is with joint holder or power of attorney on the account to monitor for suspicious transactions. Banks have made these types of

alerts easier and a trusted individual can even sign up for text alerts to receive a notification if there is a transaction that is conducted that is above a certain dollar threshold.

An additional step that law enforcement professionals may be able to take is to research and review the collectively growing database of elder financial exploitation suspicious activity reports that are reported by financial institutions, via suspicious activity reports to the Financial Crimes Enforcement Network which can assist with the initiation of new investigations, the enhancement of ongoing inquiries and potentially increase with prosecutions.

For future understanding of scam related activities, it may be pertinent for law enforcement to get a better grasp of where the funds are going that are generated as a result of scam activities. Currently, one of the most difficult aspects of scam activities that target all individuals, not just the elder population is the fact that we are not 100% sure where the funds go from any given scam, or who is even conducting the scam. From the author's own experience and knowledge the scams are sometimes conducted by a small group of individuals who are looking to make a quick buck. However, this activity can also be conducted by large organizations that are targeting hundreds of thousands of individuals and make millions of dollars that leave the United States and can go to groups that are funding terrorist groups or drug cartels. The truth is that we just do not know.

Not only is the depth of understanding of where the funds go is what is terrifying, but the fact that we do not even know how bad the victimization is. The true loss, the true hardship, and the true comprehension of these types of cases is still largely not known.

References

- Acierno, R., Hernandez, M. A., Amstadter, A. B., Resnick, H. S., Steve, K., Muzzy, W., & Kilpatrick, D. G. (2010). Prevalence and correlates of emotional, physical, sexual, and financial abuse and potential neglect in the United States: The national elder mistreatment study. *American Journal of Public Health, 100*(2), 292-297. <https://doi.org/10.2105/AJPH.2009.163089>
- Acierno, R., Hernandez-Tejada, M., Muzzy, W., & Steve, K. (2009). *National elder mistreatment study* (NCJ # 226456). Washington, DC: National Institute of Justice, Office of Justice Programs, U.S. Department of Justice.
- Arndt, J. (2022, March 4). *County warns of 'new' Medicare scam targeting elderly victims*. mykenoshacounty.com. Retrieved March 30, 2022, from <http://mykenoshacounty.com/?p=14852>
- Baker, P. R., Francis, D. P., Hairi, N. N., Othman, S., & Choo, W. Y. (2016). Interventions for preventing abuse in the elderly. *The Cochrane Database of Systematic Reviews, 2016*(8), CD010321. <https://doi.org/10.1002/14651858.CD010321.pub2>
- Balar, K. (2019). *U.S. barraged by 4.8 billion robocalls in August, according to YouMail Robocall Index*. Umail.inc. <https://www.prnewswire.com/news-releases/us-barraged-by-4-8-billion-robocalls-in-august-according-to-youmail-robocall-index-300912380.html>
- Barakat, M. (2022, February 17). *Romance fraud: Looking for love in wrong place proves costly*. ABC News. Retrieved March 30, 2022, from <https://abcnews.go.com/Lifestyle/wireStory/romance-fraud-love-wrong-place-proves-costly-82958741>

- Binder, M. (2022, March 25). *Crypto scammers are filling inboxes with fake 'donate to Ukraine' emails*. Mashable. Retrieved March 28, 2022, from <https://mashable.com/article/crypto-scammers-ukraine-email-scams>
- Bischoff, P. (2020, August 26). *The United States of elder fraud—how prevalent is elder financial abuse in each state?* Comparitech. Retrieved December 7, 2021, from <https://www.comparitech.com/blog/vpn-privacy/elder-fraud-by-state/>
- Boyd, C. (2020, March 31). Christopher Boyd, lead malware intelligence analyst. *Here are the most popular robocall scams and how to avoid them*. Malwarebytes Labs. Retrieved March 19, 2022, from <https://blog.malwarebytes.com/scams/2019/11/here-are-the-most-popular-robocall-scams-and-how-to-avoid-them/>
- Burns, D., Henderson, C. R., Jr., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. *American Journal of Public Health, 107*(8), e13-e21. <https://doi.org/10.2105/AJPH.2017.303821>
- Carney, A. (2019, September 20). *Epidemiology of elder abuse and neglect*. Elder Abuse. Retrieved March 22, 2022, from <https://www.sciencedirect.com/science/article/pii/B978012815779400001X>
- Centers for Disease Control and Prevention. (2021, June 2). Fast facts: Preventing elder abuse |violence prevention|injury Center|CDC. Centers for Disease Control and Prevention. Retrieved March 16, 2022, from <https://www.cdc.gov/violenceprevention/elderabuse/fastfact.html#:~:text=What%20is%20Elder%20Abuse%3F,a%20person%20the%20elder%20trusts.>

- Cire, B. (2016). *World's older population grows dramatically*. National Institute on Aging.
Retrieved from <https://www.nia.nih.gov/news/worlds-older-population-grows-dramatically>
- Consumer Financial Protection Bureau (CFPB). (2017). *Reporting of suspected elder financial exploitation by financial institutions*, pp. 1-25.
- Deane, S. (2018, June). *Elder financial exploitation: Why it is a concern, what regulators are doing about it, and looking ahead*. Elder Financial Exploitation White Paper–SEC.
Retrieved April 6, 2022, from <https://www.sec.gov/files/elder-financial-exploitation.pdf>
- DeLiema, M., Yonashiro-Cho, J., Gassoumis, Z. D., Yon, Y., & Conrad, K. J. (2018). Using latent class analysis to identify profiles of elder abuse perpetrators. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences*, 73(5), e49-e58.
<https://doi.org/10.1093/geronb/gbx023>
- DeMarco, J. (2022, February 18). Shameless: NJ con woman admits swindling elderly victims of \$675k in 'lottery winner' scam. *Hackensack Daily Voice*. Retrieved November 3, 2021, from <https://dailyvoice.com/new-jersey/hackensack/news/shameless-nj-con-woman-admits-swindling-elderly-victims-of-675k-in-lottery-winner-scam/826323/>
- Dessin, C. (2003). Financial abuse of the elderly: Is the solution a problem? *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.461026>
- Elder Justice Act* (EJA). (2010). Administration for Community Living. <https://acl.gov/about-acl/elder-justice-act>
- Falk, N. L., Baigis, J., & Kopac, C. (2012). Elder mistreatment and the Elder Justice Act. *The Online Journal of Issues in Nursing*, 17(3).

- Federal Trade Commission (FTC). (2021, February 23). New data shows. Received 2.2 Million Fraud Reports from Consumers in 2020. Federal Trade Commission. <https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers>.
- First Orion. (2019). *Scam call trends and projections report*. North Little Rock, AK: First Orion.
- Hafemeister, T. L. (2003). Financial abuse of the elderly in domestic setting. In R. J. Bonnie & R. B. Wallace (eds.), National Research Council (US) panel to review risk and prevalence of elder abuse and neglect. *Elder Mistreatment: Abuse, Neglect, and Exploitation in an Aging America*. Washington (DC): National Academies Press (US); 2003. 13. Available from: <https://www.ncbi.nlm.nih.gov/books/NBK98784/>
- Hamp, L. F. (2003). *Elder mistreatment: Abuse, neglect, and exploitation in an aging America*. Retrieved March 30, 2022, from <https://www.ncbi.nlm.nih.gov/books/NBK98799/>
- Held, K. S. (2021, November 4). *81-year-old 'money mule' pleads guilty in romance fraud scheme*. FOX 2. Retrieved March 30, 2022, from <https://fox2now.com/news/missouri/81-year-old-money-mule-pleads-guilty-in-romance-fraud-scheme/>
- Holtfreter, K., Reisig, M. D., Mears, D. P., & Wolf, S. E. (2014, March) *Financial exploitation of the elderly in a consumer* (pp. 1-186). Washington, DC: United States Department of Justice.
- Huang, Y., & Lawitz, A., (2016). *The New York state cost of financial exploitation study*. New York: Office of Children and Family Services.

- Jackson, S. L. (2014). The shifting conceptualization of elder abuse in the United States: From social services, to criminal justice, and beyond. *International Psychogeriatrics*, 28(1), 1-8. <https://doi.org/10.1017/s1041610215001271>
- Jackson, S. L. (2015), The vexing problem of defining financial exploitation., *Journal of Financial Crime*, 22(1), 63-78. <https://doi.org/10.1108/JFC-05-2014-0026>
- Krienert, J. L., Walsh, J. A., & Turner, M. (2009). Elderly in America: A descriptive study of elder abuse examining National Incident-Based Reporting System (NIBRS) data, 2000-2005. *Journal of Elder Abuse & Neglect*, 21(4), 325-345. <https://doi.org/10.1080/08946560903005042>
- Lassoff, B. (2018, August 30). *Real case examples of financial exploitation of the elderly*. MassMutual. Retrieved March 6, 2022, from <https://blog.massmutual.com/post/financial-exploitation-seniors-massmutual>
- Legal Information Institute. (2010). *42 U.S. Code § 1397L - Establishment and support of elder abuse, neglect, and exploitation forensic centers*. Legal Information Institute. Retrieved March 6, 2022, from <https://www.law.cornell.edu/uscode/text/42/13971>
- Moore, C., & Browne, C. (2016). Emerging innovations, best practices, and evidence-based practices in elder abuse and neglect: A review of recent developments in the field. *Journal of Family Violence*, 32(4), 383-397. <https://doi.org/10.1007/s10896-016-9812-4>
- National Adult Protective Services Association (NAPSA). (n.d.) *Exploitation resources*. Napsa-now.org. Retrieved March 26, 2022, from <https://www.napsa-now.org/get-informed/exploitation-resources/>

National Committee to Preserve Social Security and Medicare (NCPSSM). (2021, March 23).

Older Americans Act. Retrieved March 19, 2022, from <https://www.ncpssm.org/documents/older-americans-policy-papers/older-americans-act/>

National Council on Aging (NCOA). (2021, February 19). Top 10 financial scams *Targeting Seniors*. <https://www.ncoa.org/article/top-10-financial-scams-targeting-seniors>.

National Research Council (US) Panel to Review Risk and Prevalence of Elder Abuse and Neglect, Bonnie, R. J., & Wallace, R. B. (Eds.). (2003). *Elder Mistreatment: Abuse, Neglect, and Exploitation in an Aging America*. National Academies Press (US).

NBC Universal News Group. (2021, November 11). *Florida woman, 82, loses more than \$700,000 in 'grandparent scam'*. NBCNews.com. Retrieved December 8, 2021, from <https://www.nbcnews.com/news/us-news/florida-woman-82-loses-700000-grandparent-scam-rcna5235>

Otto, J. M. (2000). The role of adult protective services in addressing abuse. *Generations: Journal of the American Society on Aging*, 24(2), 33-38. <http://www.jstor.org/stable/44878439>

Pillemer, K., Burnes, D., Riffin, C., & Lachs, M. S. (2016). Elder abuse: Global situation, risk factors, and prevention strategies. *The Gerontologist*, 56(Suppl 2), S194-S205.

<https://doi.org/10.1093/geront/gnw004>

Rhode, M. (2022, April 1). *Retired teacher loses \$45,000 in Gift Card Scam*. AARP. Retrieved March 30, 2022, from <https://www.aarp.org/money/scams-fraud/info-2022/retired-teacher-loses-thousands.html>

United States Department of Health and Human Services (HHS). (2016, March 28). *World's older population grows dramatically*. National Institutes of Health. Retrieved March 30,

2022, from [https://www.nih.gov/news-events/news-releases/worlds-older-population-grows-dramatically#:~:text=The%20world's%20older%20population%20continues,by%202050%20\(1.6%20billion\).](https://www.nih.gov/news-events/news-releases/worlds-older-population-grows-dramatically#:~:text=The%20world's%20older%20population%20continues,by%202050%20(1.6%20billion).)

United States Department of Justice (DOJ). (n.d.). *Elder abuse and elder financial exploitation statutes*. Retrieved March 13, 2022, from <https://www.justice.gov/elderjustice/prosecutors/statutes?page=10>

United States Department of Justice (DOJ). (2019, October 31). *Pawtucket man sentenced in international scam targeting the elderly*. Retrieved March 6, 2022, from <https://www.justice.gov/usao-ri/pr/pawtucket-man-sentenced-international-scam-targeting-elderly>

United States Department of Justice (DOJ). (2020, March 3). *Attorney general William P. Barr announces the results of the Department of Justice's 2020 elder fraud sweep and New Nursing Home initiative*. Retrieved March 30, 2022, from <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-results-department-justices-2020-elder-fraud>

United States Department of Justice (DOJ). (2020, October 30). *Owner of Minnesota and California magazine sales companies pleads guilty to conspiracy to commit mail fraud*. Retrieved March 18, 2022, from <https://www.justice.gov/usao-mn/pr/owner-minnesota-and-california-magazine-sales-companies-pleads-guilty-conspiracy-commit#:~:text=United%20States%20Attorney%20Erica%20H,District%20Court%20in%20Minneapolis%2C%20Minnesota.4>

Weisman, A. L. (2020, March 3). Department of justice charges unprecedented number of elder fraud defendants and launches hotline. The United States Department of Justice.

Retrieved March 16, 2022, from <https://www.justice.gov/usao-ri/pr/departement-justice-charges-unprecedented-number-elder-fraud-defendants-and-launches>

WLOS. (2022, March 16). *Scam alert: Stolen cryptocurrency returned to Asheville man in government imposter case*. WLOS. Retrieved March 30, 2022, from <https://wlos.com/news/local/cryptocurrency-scam-north-carolina-asheville-attorney-general-inspector-beware-fbi>

Wolf, R. (2003). *Elder mistreatment: Abuse, neglect, and exploitation in an aging America*.

Retrieved March 23, 2022, from <https://www.ncbi.nlm.nih.gov/books/NBK98805/>

World Health Organization. (n.d.). Elder abuse. World Health Organization. Retrieved March 16, 2022, from <https://www.who.int/news-room/fact-sheets/detail/elder-abuse#:~:text=Elder%20abuse%20is%20a%20single,distress%20to%20an%20older%20person.>

Yon, Y., Mikton, C. R., Gassoumis, Z. D., & Wilber, K. H. (2017). Elder abuse prevalence in community settings: A systematic review and meta-analysis. *The Lancet. Global Health*, 5(2), e147-e156. [https://doi.org/10.1016/S2214-109X\(17\)30006-](https://doi.org/10.1016/S2214-109X(17)30006-)

Bibliography

- Administration for Community Living. (2017, September 27). *The Elder Justice Act*. ACL Administration for Community Living. <https://acl.gov/about-acl/elder-justice-act>
- Civil Financial Exploitation. (2020). 10 G.C.A. § 21002. *Definitions*.
- Congress.gov. (1991). Vulnerable Elders' Rights Protection Amendments of 1991. H.R. 2864. 102nd Congress.
- Department of Justice. (2019, September 23). Senior scam alert. The United States Department of Justice. <https://www.justice.gov/elderjustice/senior-scam-alert>
- Downey, T. J. (1991, April 24). Elder abuse: Effectiveness of reporting laws and other factors. United States General Accounting Office. Report to the Chairman, Subcommittee of Human Services, Select Committee on aging, House of Representatives.
- Elder abuse statistics—Statistics on elderly abuse over time*. (n.d.). Nursing Home Abuse Center. [sdhttps://www.nursinghomeabusecenter.com/elder-abuse/statistics/](https://www.nursinghomeabusecenter.com/elder-abuse/statistics/).
- Federal Bureau of Investigation. (2020, June 15). *Elder fraud*. FBI. <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud>.
- Federal Communications Commission (FCC). (2012, May 25). *Watch out for 'grandparent' scams*. Retrieved March 16, 2022 from <https://www.fec.gov/watch-out-grandpaarent-scams>
- FindLaw. (2021, May 17). Elder financial abuse and exploitation. Findlaw. <https://www.findlaw.com/elder/elder-abuse/elder-financial-abuse-and-exploitation.html>
- Internet Crime Complaint Center, & FBI. Elder Fraud Report 20201-22. (2020). FBI.

- Maxwell, A. (2021, December 3). *Jacksonville veteran says he's victim of a social media romance scam*. WJXT. Retrieved December 7, 2021, from <https://www.news4jax.com/news/local/2021/12/03/jacksonville-veteran-says-hes-victim-of-a-social-media-romance-scam/>
- Office of Justice Programs. (2017). *K. Holtfreter, M. D. Reisig, D. P. Mears, and S. E. Wolfe, Final report: financial exploitation of the elderly in a consumer context* 1–186. Phoenix, AZ: National Institute of Justice.
- Patient Protection and Affordable Care Act. (2010).
- Phelan, A. (2020). *Advances in elder abuse research*. Springer International Publishing.
- Press, T. A. (2022, February 21). *Elderly man swindled out of \$500k in romance scam*. WFLA. Retrieved December 15, 2021, from <https://www.wfla.com/news/crime/elderly-man-swindled-out-of-500k-in-romance-scam/>
- Research Statistics and Data. NCEA. (n.d.). https://ncea.acl.gov/What-We-Do/Research/Statistics-and-Data.aspx#_ednref27
- Statistical Research Department. (2021, January 20). *U.S. population by age and gender 2019*. Statista. <https://www.statista.com/statistics/241488/population-of-the-us-by-sex-and-age/>
- The National Council on Aging (NCOA). (2021, February 23). *Get the facts on elder abuse*. Retrieved March 6, 2022, from <https://www.ncoa.org/article/get-the-facts-on-elder-abuse>
- Trevor John Mills, M. D. (2020, June 30). *Elder abuse*. Background, Epidemiology. <https://emedicine.medscape.com/article/805727-overview#a5>
- Wolf, R. (2003). Elder abuse and neglect: History and concepts. In: National Research Council (US) Panel to Review Risk and Prevalence of Elder Abuse and Neglect. R. J. Bonnie and

R. B. Wallace, editors. *Elder mistreatment: Abuse, neglect, and exploitation in an aging America*. Washington (DC): National Academies Press (US); 2003. APPENDIX C.

<https://www.ncbi.nlm.nih.gov/books/NBK98805/>