BULLSEYE: THE ELDERLY COMMUNITY, A PERFECT TARGET FOR ONLINE SCAMMERS

Leann McClain

About the Author

My name is Leann McClain. I am a current graduate student in the Interdisciplinary Program. I have a Bachelor of Arts Degree in English Writing and Literature with a Minor in History. I want to thank a few people for the publication of this paper. First, I would like to thank Dr. Sridhar Ramachandran. In the Fall of 2024, I took his course Cyber and Legal Security, and I wrote this paper. Dr. Ramachandran encouraged me to submit this paper. I would also like to thank my family members and friends. The constant support, love, and encouragement I receive from them allows me to continue to follow my dreams. I dream that one day I can reach people far and wide with my writing.

RESEARCH AIMS AND OBJECTIVES

Imagine that you and your spouse have worked hard for many years. Doing everything possible to grow a family, make your house a home, and save money for both of you to retire. The time comes when the children who have all grown up leave the house and have children of their own. Now is the time for you and your spouse to take your savings and live out your twilight years together. Suddenly, one day, everything is gone. The entirety of your livelihood has vanished within one phone call. In February of 2024, this was the reality for elderly couple Gloria and Gary Moss of Deluth, Atlanta. On February 16, 2024, the couple received two texts from Chase Bank Fraud department claiming Gary's Chase Bank card was compromised. Upon receiving the message, Gloria

Moss called the number. Describing the phone call, Gloria said, "The sales rep was very professional and was told that her husband's debit card was used at a retailer in another state at a retailer with a subtotal of $4,000 (Fowle, 2024)." Moss quickly disputed the charges and was prompted to answer more questions such as her card number, social security number, and to verify her cellphone. The Mosses would lose their entire life savings of $49,000 in a twenty-minute phone call. The Mosses story is only one of many people who get conned by scammers every day. According to the National Consumer Law Center in 2022,68 million Americans lost over 29 billion to scam callers. As technology advances and evolves, scammers are going to be a larger problem, and the elderly community is going to be a vulnerable target. The research aims and objectives of this paper are to review current literature about:

- How scammers target the vulnerable elderly community.
- Current solutions that are being used to combat the problem.
- What future steps can be taken in the field of cybercrime and security to protect the elderly community from being victimized by scammers.

LITERATURE REVIEW

The above story about the Moss couple is just one of many instances where spammers have used the vulnerability of the elderly to get what they can out of them at a devastating cost. In 2021, Steve Price wrote an article, "Stop the Calls: Robo Callers Trick Grandmother Out of Life Savings," which involved eighty-two-year-old Marjorie Jones, who took her own life after losing the entirety of her life savings to phone scammers masquerading as representatives from government agencies. During a congressional hearing, Jones' granddaughter testified in the aftermath of her grandmother being a victim of scammers, which resulted in a reverse mortgage on her home, and dying with only $69.00 in her bank account. While the government knows that older adults are unfortunately targeted or disproportionately affected by robocall scams; the US has not figured out how to adequately regulate them. Hearing these

devastating stories about the ability to lure and take advantage of senior citizens raises the question of why they become such vulnerable targets for scammers. Over the last thirty years, studies have been conducted to figure out the vulnerable link between senior citizens and scammers.

The literature that will be reviewed and discussed in this paper is broken down into three parts. The first part will consist of a review of studies that attempt to focus on the elderly community and what makes them a vulnerable target for scammers. These studies take technological, behavioral, and phenomenological approaches, providing readers with insight into the issue of the elderly community being vulnerable to scammers. The second aspect of this paper discusses the current government actions in place to combat the scammers. This section also covers the technological art of scambaiting. A technological niche that has grown on YouTube in the last decade involves influencing scammers behind various scams and using various techniques to waste their time, catch them in the act, and even tracking and shutting down scammer companies. The third and final aspect will concentrate on the future solutions of scammers and ways to eliminate their attacks on the elderly community.

2.0 The Elderly Community: Scammers Vulnerable Targets

The above story about the Moss couple is just one of many instances where scammers have used the vulnerability of the elderly to get what they can out of them at a devastating cost. In 2021, Steve Price wrote an article, "Stop the Calls: Robo Callers Trick Grandmother Out of Life Savings," about eighty-two-year-old Marjorie Jones who took her own life after losing the entirety of her life savings to phone scammers masquerading as representatives from government agencies. During a congressional hearing, Jones's granddaughter testified that her grandmother had taken a reverse mortgage on her home and died with only $69.00 in her bank account. These devasting stories from the Mosses and Majorie cases remind us of

how badly scam calls can impact a person's entire livelihood in one phone call or text message. Complaints of robocalls and spam call complaints were number one on the Federal Communications Commission (FCC) 2020 complaint list. While the government knows that older adults are unfortunately targeted or disproportionately affected by robocall scams the US has still not figured out how to adequately regulate them. Hearing these devastating stories about the ability to lure and take advantage of senior citizens raises the question: "How do senior citizens become such vulnerable targets for spammers?" Over the last thirty years, there have been studies conducted to figure out the vulnerable link between senior citizens. In the article titled, "Fraudsters Target the Elderly: Behavioral Evidence from Randomized Controlled Scam-Baiting Experiments," Robinson and Edwards (2024) conducted a study which displayed how senior citizens can become tricked into various scambaiting scenarios. Prior to their own study, they found that the consensus in previous studies was that being lonelier, friendly, and trusting are the most identified characteristics affecting an individual's susceptibility to scambaiting. They also found that some of these studies have conflicting views because of lower reports of self-reported scam victimization, the perception can be skewed. Victims may feel embarrassed or do not see their loss as significant.

2.1 The Behavioral Scambaiting Study: Fraudsters Target the Elderly

Authors Robinson and Wilson aimed to conduct a study addressing a key question in online fraud research: What factors do fraudsters find appealing in potential victims? To do this, they first conducted a public perception of 92 people and asked them to identify which factors would be a target for falling for scams. The initial participation survey results are demonstrated in the image below.

Factor	Being targeted			Being victim		
	Lesser (%)	No effect (%)	Greater (%)	Lesser (%)	No effect (%)	Greater (%)
Age (older)	1.1	26.1	72.8	2.2	38	59.8
Education (higher)	33.7	66.3	–	34.8	64.1	1.1
Previous exposure	43.5	33.7	22.8	58.7	21.7	19.6
Personality (kindness)	–	53.3	46.7	–	30.4	69.6

Participants were asked to choose from four different personality choices: Old Woman Doris, Naïve Youth Alex, Rude Middle Aged Man Dave, and Professional Businessperson Sam. Results from the perception survey found that participants overall who carry a higher risk being targets and falling victim to online fraud scams was the older group personalities (Robinson & Wilson, 2024). Robinson and Johnson took their findings and realistically tested them by designing an experimental automated scambaiting platform with four instrumental personality types.

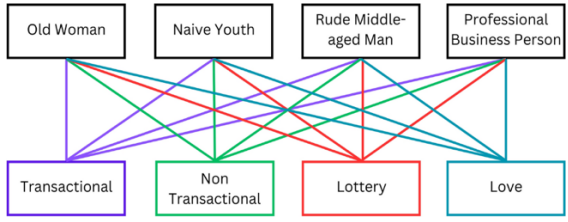

Figure 1: Illustration of the four distinct personalities' design and the various scams they were responding to.

The above image shows an example of the design that Robinson and Wilson (2024) created of the four distinct personalities and the scams they were going to be used for. In the latest designs, they named their distinct personalities as Old Woman Doris, Naïve Youth Alex, Rude Middle-Aged Man Dave, and Professional Business Person Sam. The experiment took place over the span of a month and the personality reply system contacted real scammers. One of the interesting aspects of their experiment was the conversation length by replier. The two personality designs that held the longest conversation lengths were Naïve Youth Alex, with 32 rounds of

conversation, followed closely by Old Woman Doris, with 30 rounds of conversation. This is illustrated in the image below.

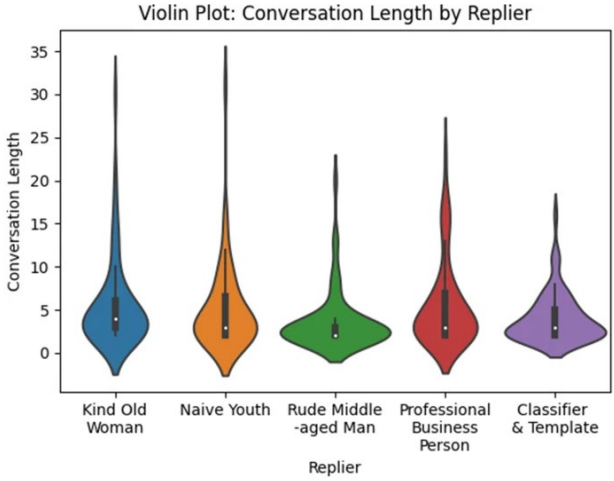

Figure 2 A violin plot to show the distribution of data with respect to conversation lengths per replier.

In their findings, Robison and Johnson found that Kind Old Woman Doris was the best performer at conversation length (Robinson & Johnson, 2024). It would make sense that Old Woman Doris has the behavioral traits of being gullible and having a trusting nature which is what makes her vulnerable to scammers. While the study presents a basic behavioral perspective displaying how scammers choose their targets, and the conversational tactics they use, the study only worked within the basis of e-mail type frauds. Future studies could expand their findings into telephone-type scams. By doing this, they would have a more rounded perception of why elderly people are the primary target for scams. Future studies could also design their personalities to contrast with those of others in their age group. Personalities like Kind Old Woman Doris, were designed and presented as having reactions from one personality. In future studies, it would be beneficial to see different responses from people

of the same age group. To conclude the findings of their study, Robinson and Johnson noted the behavioral evidence they found from both the scammers and the personalities they designed was that scammers are more likely to engage and persist with targets they believe are elderly (Robinson & Wilson, 2024). This prompted Robinson and Wilson to wonder if a countermeasure could be put in place to teach the elderly about the dangers of spam calls and fraud.

2.2 Cognitive Decline and Spam Vulnerability Among Elderly Adults Study

The study conducted by Robinson and Wilson focused on certain personality and behavioral traits that attracted scammers, which provides insight into why the elderly community is targeted by scammers. In 2021, psychiatrists and mental health specialists in various areas of Japan came together and conducted a study which would attempt to answer the question of whether cognitive decline is a risk factor for vulnerability in older adults. The study began with the creation of a scam vulnerability scale survey with participants of 50 years and older, each with a different variation of cognitive decline. The average age of these participants was 79.42 years old. Then, the team began another study involving 51 adults without cognitive decline. The average age was 76.12 years old. The referenced table is illustrated below.

Table 1

	CD	CND	*p* value
Age	79.4	76.1	0.004**
Sex (female)	35	27	0.078[n.s.]
Psychosocial factors			
Years of education	12.6	13.6	0.043*
SES[a]	4	4	0.171[n.s.]
Living style with family [b]	3	3	0.855[n.s.]
Income satisfaction	3.4	3.3	0.341[n.s.]
Frequency of going out [a]	1	1	0.537[n.s.]
Ability for viewing [c]	3	3	0.602[n.s.]
Ability for hearing [c]	1	1	0.707[n.s.]
IADL[d]	4	5	0.205[n.s.]
UCLA	30.5	28.7	0.304[n.s.]
GDS-S	3	4	0.527 [n.s.]
MSPSS	66.2	64.2	0.467[n.s.]
Neuropsychological factors			
MMSE	24.0	28.8	<0.001***
SDMT	34.1	43.4	<0.001***
RBMT-SS	4.9	8.2	<0.001***
Fluency-Letter	8.2	11.0	<0.001***
-Category	11.0	14.1	0.001**
J-EXIT25	11.2	7.3	<0.001***
ADAS-Jcog	11.2	4.8	<0.001***
CDT-Free	7.5	8.0	0.120[n.s.]
CDR[e]	0.5	0.0	<0.001***
Decision-making			
Emotional framing[b]	4	2	<0.001***
Risk framing (gain domain)[b]	2	2	0.034**
Risk framing (loss domain)[b]	1	1	0.349[n.s.]

SES, Socio-economic status scale; IADL, Instrumental activities of daily living scale; UCLA, University of California at Los Angeles loneliness scale; GDS-S, Geriatric depression scale-short version; MSPSS, Multidimensional Scale of Perceived Social Support; MMSE, Mini-mental state examination; SDMT, Symbol digit modalities test; J-EXIT25, Japanese versions of the executive interview; ADAS-Jcog, the Japanese version of the Alzheimer's disease assessment scale-cognitive subscale; CDT, Clock drawing test; RBMT-SS, Rivermead behavioral memory test-screening score. [a] Median; [b] Mode; $^{**}p < 0.001$, $^{**}p < 0.01$, $^{*}p < 0.05$, [n.s.] not significant.

Table 1. Characteristics of participants in the cognitive decline (CD) and cognitive non-decline (CND) groups.

After the interview, participants went through a series of neuropsychological tests to evaluate their cognitive function. Some tests used included the clock drawing test, the verbal fluency test, and the Riverhead Behavioral Memory test. These tests are used to diagnose cognitive diseases such as Alzheimer's, and dementia. The findings conducted from the tests, and the scam vulnerability scale, allowed the specialists to conclude that older adults with mild cognitive decline are more susceptible to scams. Older adults with moderate to severe cognitive decline may have difficulty understanding situations, thus giving scammers an opportunity to maliciously fill gaps with information benefiting them (Frontiers, 2024). The results of this study provided insights into cognitive decline and fraud vulnerability in older adults. The authors found that mild cognitive decline in global cognitive function is a risk factor in scam vulnerability in older adults (Frontiers, 2024). The limitations in this study were that they did not examine all risk-related factors psychosocial characteristics, such as the participant's personality. Another limitation was the difference between fraud scam vulnerability versus victimization. Their study focused solely on fraud vulnerability. Future studies should focus on the effect of scam victimization on older adults with a cognitive decline. While

the first study by Robinson and Johnson used a technological focus on the behavioral vulnerability of elderly people being targeted by scammers. This study concentrated more on the health aspects of cognitive decline in older adults and why they are susceptible to scams.

2.3 Older Adults and Underreported Scams: A Phenomenology Study

Authors Katalin Patri and Faika Tahir wanted to find out exactly why older individuals are highly susceptible to scams. In the article "If We Don't Listen to Them, We Make Them Lose More Money," a study was conducted using a phenomenological approach to identify why older individuals decide not to report scams and to explore the needs of victims. The study involved thirty-five interviews with Virginia residents who were 60 years or older as of 2021. Patri and Tahir conducted various types of sampling to gather interviewees. They found the snowballing method was the most effective for recruiting interviewees who had been victims of a scam because once a person has been a victim of a scam, they often lack trust in the phone or computer. The authors asked other people interviewed to reach out to others who were victimized by spammers. The interviews lasted between 15-72 minutes. Of these individuals 22 identified as female and the remaining 13 identified as male. One interviewee was African American, while the other interviewees were Caucasian. During the interview process, most participants discussed other people's experiences of spam victimization, while others talked about their own experiences. An interesting aspect that was found during this study was Despite the fact that not everyone was victimized every participant was indeed approached by scammers multiple times via either phone, computer, or social media (Patri & Tah, 2023). The information collected in the interviews was then grouped together into different codes. The codes were divided into three large categories as illustrated below.

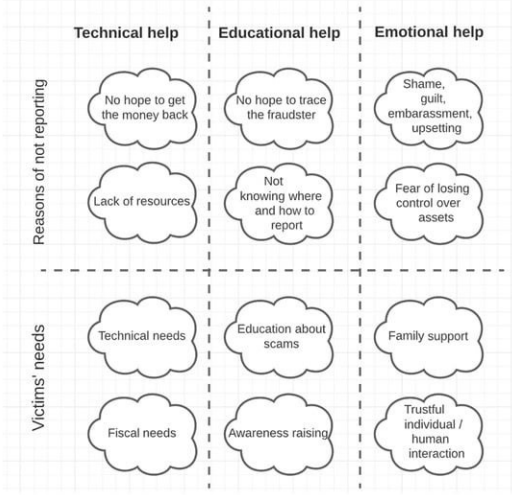

Figure 4 1Main Codes of Underreported Scams in older Adults

Although interviews were conducted on a phenomenological level, Patri and Tahir (2023) were able to gain a bigger perspective on the psychological and emotional impact that scams have on people. The biggest barriers that prevented a victim of a scam from reporting it were emotional, educational, and technical issues. They found that when it comes to asking for help or reporting an incident, a victim's thought process is not entirely rational (Patri & Tahir, 2023). The study also found that the emotional and psychological impact can be more stressful than the impact of what a victim loses financially. The limitations of this study begin with where the interviews took place in the Commonwealth of Virginia without focusing on personal characteristics apart from the fact that the interviewees were all over the age of 65. The interviewees in the study do not represent a diverse population of people, and half of the participants acted as secondary informants from the victim's family or friend group. Given the information shared in the interviews, it proves how difficult it is to find scam victims willing to share their stories. Although the authors' choice to conduct the study from a

phenomenological approach provided a voice to those who were victimized, the samplings of the study were so small they could not be generalized. In future studies, the authors recommend providing more diverse demographics.

The first three studies in this paper use behavioral, psychological, and phenomenological approaches to provide insight into why scammers are a problematic target for the vulnerable community of the elderly. Each study has its own diverse methods; however, all three seem to be of similar agreement that future studies need to focus on methods of awareness and to provide technical and emotional help for the elderly community regarding falling victim to future scams.

3.0 Combating Scammers: Preventative Actions Currently in Place

The earlier section of this paper attempted to answer the question of: Why is the elderly community such a vulnerable target for scammers? As we have looked in previous studies, there are technological, psychological, and social aspects as to why scammers see the vulnerability of the elderly community as a perfect target. While scammers are a huge issue for everyone, the previous studies and literature have shown us that a lack of technical knowledge and awareness of these scams, being too trusting, and dealing with cognitive issues are the main reasons why once targeted, the elderly community stands to lose so much more to scammers from their financial livelihood to even their lives. Now that the problem has been established, we must now investigate what is currently being done to combat the problem.

3.1 The Telephone Protection Act of 1991 and It's Criticism

The Telephone Protection Act (TCPA) was signed into law in 1991. The law protects people from receiving certain types of unsolicited telephonic communications (Egan, 2022). The TCPA

was originally created to stop telemarketers from placing bothersome calls to residential landlines. Today, the law extends to protection from robocalls and/or Automatic Telephone Dialing System (ATDS). The TCPA is not without criticism, especially its use and protection in today's technological landscape.

Author Nicole Egan offers such criticism in the article titled, "Rage Against the Machine: Reducing Robocall Abuse to Protect At-Risk Consumers." Egan discusses two different court cases: *Duguid vs. Facebook, Inc,* and *Duran vs. La Boom Disco.* In both court rulings, the plaintiffs had to deal with numerous unsolicited messages being sent to them. In the *Duguid vs. Facebook, Inc.* case, the plaintiff sued Facebook after repeatedly receiving automatic two-factor authorization texts from the company. The company sent out texts claiming that Mr. Duguid had been accessing his Facebook. Mr. Duguid never had a Facebook account to begin with (Egan, 2024). Mr. Duguid filed a suit and claimed that these messages he apparently sent were a violation of the TCPA because the texts were being sent without his consent. The court disagreed with his ruling.

Another case that had similar results was *Duran V.S. La Boom Disco.* The plaintiff, Duran, claimed that he was sent numerous unsolicited text messages from the nightclub. Although the nightclub owner was accused of violating the TCPA by sending hundreds of unsolicited texts to the plaintiff, the district court found the messages to be lawful because they had not been sent by an ATDS (Egan, 2022). Similarly, in the Duguid case, the court ruled in favor of Facebook stating that Facebook's system was not restricted to the language of the TCPA. Egan discussed the outcome of these two cases and criticized the court's ruling, saying in deciding that Facebook's system was not restricted to the language of the TCPA, the court limited the scope in what may actually be considered an ATDS and potentially provided yet another workaround for scammers to exploit" (Egan, 2022). By describing and covering the outcome of these two cases regarding the TCPA, Egan showed that the TCPA is being looked at too narrowly by the

Supreme Court. The courts are focusing on the wrong aspect when looking at the rules of the TCPA. The ruling still comes from a 1991 landscape, and they need to broaden the scope to fit the social media landscape of today.

3.2 The National Do Not Call Registry

People began using cell phones as early as the 1970s, but their popularity grew in the early 2000s. As cell phones became more popular, so did spam calls. In response to this, the FTC created the 'National Do Not Call Registry' in 2003. Consumers who added their numbers to the registry were guaranteed they would not be contacted by telemarketers (CBS,2021). Over the next few years, the 'National Do Not Call Registry' would not be as effective against the influx of spam and robocalls that consumers would continuously receive. The 'National Do Not Call Registry' was successful against telemarketers because telemarketers were actual human beings dialing the numbers of consumers hoping to talk to them. Telemarketing companies wanted to avoid penalties for breaking the law. Spam and robocalls are very different from human telemarketers. While there may be an actual person causing an automated system to make robocalls, finding the identity of the person is extraordinarily difficult because their identity and location are shielded by modern auto-dialing technology. In 2020, The FTC collected over 3.9 million complaints from people whose numbers were listed on the registry but were receiving calls anyway (FTC, 2020). While it had good intentions, when it was first enacted, the 'National Do Not Call Registry' failed to keep up with the constant influx of spam and robocalls. In recent years, the government has investigated more efficient methods.

3.3 ***The Stir/Shaken Framework***

In 2021, the FCC developed a new measure designed to decrease the number of phone calls consumers received called the STIR/SHAKEN framework. This framework requires phone

carriers to authenticate the identification of a caller before the call even reaches the consumer's phone. It also erodes the ability for callers to fake a caller ID, which masks the callers' identity and tricks people into answering a call. According to the FCC, if the call does not originate from a STIR/SHAKEN framework-compliant provider, the call will be blocked (Egan, 2022. The STIR/SHAKEN framework operates by requiring carriers to check the legitimacy of the caller's identity or risks having calls originating from their networks be terminated or blocked for failure to comply, which would negatively affect the phone company's business. The STIR/SHAKEN framework went into effect in June 2021, and the number of spam and robocalls received that summer dropped by 29% when compared to June through August of the previous year (12 news, 2021). One aspect of the STIR/SHAKEN framework provides users with a series of alerts representing various states of authentication in incoming calls. In 2021, a study was conducted on this aspect of the framework. In the article titled "Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard," the authors wanted to know how clear these alert authorization notifications were to the consumer. The study aimed to find out how carriers react to specific authentication types, evaluate the interpretation of warning designs of the STIR/SHAKEN authentication states, and then how users plan and interpret these different states.

The methodology that the researchers used in this study was a combination of surveys and interviews. There were 806 participants divided between Mturk Crowdsource Workers and The National Federation for the Blind. The researchers first studied the response to incoming calls. Mturk and The National Federation for the Blind (NFB) participants were asked to respond to two of six incoming call screenshots (Sherman, 2021). The participants were then asked a series of questions about how they preferred specific types of information to be and how they wanted to be notified. In their study, the researchers found that the STIR/SHAKEN framework can be a useful method; however, when usability is an afterthought,

consumers often suffer, and technology can be ineffective if consumers do not know how to use it (Egan, 2022). Although the STIR/SHAKEN method is a good initiative as of right now, it only appears to work well with Voice Over Internet Protocol (VOIP) calls. With the evolution of technology, scammers can utilize not only on the telephone but also emails and social media sites.

3.4 Scambaiting: You Tube's Effective yet Entertaining Social Media Subgenre

In May of 2022, The Times of India published the article titled, "How Four International Sleuths Teamed Up to Expose Call Centre's in Kolkata," which discussed how YouTube influencers such as Mark Rober, Trilogy Media, and Jim Browning used various pranks and hacking skills to track down and take down scammer call centers. Rober, Trilogy Media, and Jim Browning are part of an entertaining yet informative niche on YouTube known as scambaiting, which is defined as the practice of pretending to fall for fraudulent online schemes to waste the time of perpetrators (Collins, 2024). Typing 'scambaiting' into the YouTube spacebar will provide users with many videos of various YouTubers messing with scammers by changing their voices, irritating them, and keeping them on the call for as long as possible. As entertaining as 'scambaiting' can be, it can also be effective. Mark Rober, an ex-NASA engineer turned YouTuber, began receiving scam calls. He decided to dig deeper and track down their origins. When he found out that most of the calls came from India, he teamed up with other YouTubers known as Jim Browning and Trilogy Media for a year-long collaboration to investigate these fake call centers.

The findings of the investigation were released in a viral video on Rober's YouTube titled, "Pranks Destroy Scam Callers: Glitter bomb Payback." To date, the video has gained 103 million views, and the collected evidence helped police track down and shut down these call centers. Jim Browning helped the team zero in on the four call centers in the video infiltrated and gained access to the Closed-

Circuit Television (CCTV) camera feeds and computers. Then, they found two reformed agents who used to work at these call centers who knew people on the inside. They began providing information on how things work, so it was like a puzzle that took us years of investigation to put together (India Times, 2024). After they had collected enough information, the YouTube team then sent their undercover agents to the Kolkata Call Centers to put the prank glitter bomb devices that they had designed in place. Once the scammers opened the box, they would be met with a face full of glitter, stink bombs, cock roaches, and even rats. Although the pranks can be funny, Rober said glitter bombs and cockroaches were funny and harmless and just a means to an end. How do we make something entertaining while shining a spotlight on this damaging situation that is ruining people's lives? (India Times, 2023).

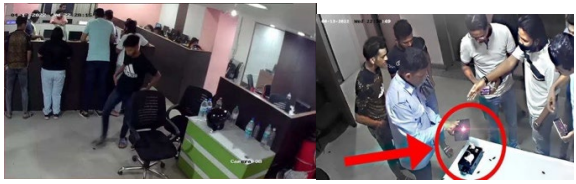

Figure 4 2CCTV FEED of Scammer Offices

The information that Rober, Browning, and Trilogy Media collected was shared with the Kolkata police, resulting in the closure of these call centers. However, the problem continues. Mumbai-based cybercrime investigator Ritesh Bhatia stated such call centers have been mushrooming all over India especially in areas of Delhi, NCR, and Dubai. These call centers do legitimate business by day and illegitimate business by night, which is why it is so hard to demolish the problem for good (India Times, 2024). The subgenre of 'scambaiting' is still growing on YouTube. At the same time, it is still hard to demolish scammers and their base of operations. YouTubers such as Rober, Trilogy Media, Jim Browning, Scammer Payback, and many others will continue to use their platform to find ways to mess with scammers by wasting their time, deleting their files, or getting them to shut down. The sharing

and discussions on scambaiting videos on YouTube will hopefully bring awareness to people on the different types of scams and how to avoid them, especially for the elderly community and their families.

The overall focus of the section of this paper was to discuss preventative actions that were currently in place against scammers, and how individuals are using social media platforms such as YouTube with their own skills in computer technology to bring awareness of scammers. Each current action is not without its own limitations. The Telephone Protection Act of 1991 was enacted to combat telemarketers and with the growth and development of today's technology. The act is no longer effective, and moving forward, the act needs to be looked at and changed. While the art of scambaiting can be effective, it has also been criticized. Comments on the YouTube videos and Reddit have questioned whether the videos by some of the scambaiters are real. While some scambaiters have managed to get some call centers shut down, new ones continue to pop up, and by parading as a legitimate business, they are hard to track and close. The limitations that this act as well as scambaiting pose need to be looked at as technology continues to grow.

4.0 Future Resolutions for Safeguarding the Elderly Community Against Scammers

The first two sections of this paper brough forth the issue of how the elderly population is such a vulnerable target for scammers, the reasoning behind this, as well as the current protection that is in place why that is, and current protections that are in place. Moving forward, we look to the future of potential resolutions that can help the elderly community against scammers.

4.1 Ban the Sale of Personal Data

Thus far, we have reviewed the current literature on protective acts in place to keep scammers at bay, as well as the challenges they still

pose for consumers, especially in the elderly community. Now we need to look into future resolutions that will keep consumers safe from scammers and scams. One resolution would be to ban the sale of personal data. A question that was left out in the case of *Duguid V.S. Facebook Inc. was how exactly Facebook attained Mr. Duguid's number in the first place.* Mr. Duguid's number may have been picked up by a data broker. Data brokers make huge profits from selling phone numbers and other personal information to a variety of companies. Consumers unwittingly give companies permission to sell data all the time without even thinking about it, usually by agreeing to a buried clause in the website's terms and conditions. The terms are usually in print so small that no one ever bothers to read them if they can even find them (Wagner, 2022). Technology can already be difficult for the elderly community to navigate through. There needs to be more protection and awareness brought to the elderly community about the tactic's scammers can use, not just over the telephone but on social media as well.

4.2 Multipronged- Cybersecurity Analysis

Amirrul and Zukry (2024) conducted a study that identified and evaluated multifaceted strategies to improve digital literacy, create user-friendly digital banking interfaces, enact and enforce strict regulator frameworks, and encourage senior citizens to feel comfortable using electronic banking. The methodology introduced in their article, "Strategies for Protecting Senior Citizens Against Online Banking Fraud and Scams: A Systematic Literature Review," was designed to identify, evaluate, and synthesize all relevant research involving senior citizens and banking fraud. Several studies were evaluated and compiled to generate the following questions:

- RQ1: What methods are effective in safeguarding senior citizens in online banking from fraud and scam activities?

- RQ2: How do demographic factors (such as age, education level, and IT proficiency) influence the effectiveness of different safeguarding methods for senior citizens in online banking?
- What role do financial institutions and technology providers play in enhancing the online banking security of senior citizens and how can their efforts be optimized?

The research also included strategies for keyword searches, selected databases, and criteria for including or excluding certain literature. The questions above and the study framework created allowed the authors to illustrate how studies were categorized and the findings from previous studies that were relevant to their questions. By researching and reviewing previous studies, they found that the most effective methods for safeguarding senior citizens in online banking in the future was a combination of educational programs focused on digital literacy, the development of user-friendly digital interfaces, regulatory reforms aimed at protecting vulnerable users (Ammirr, 2024). In the future, when it comes to safeguarding the elderly against scammers or fraudulent activity, there needs to be collaboration amongst policymakers, financial institutions, technology developers, and community organizers in addressing the technological, educational, and legislative dimensions of cybersecurity for senior citizens.

Conclusion

This paper's aim was to discuss the problem of the elderly being a vulnerable target for scammers. In section one, we discussed how and why this happens using studies that provide a technological, psychological, and phenomenological approach. These studies are good at providing readers with a foundation of the issue the elderly community can face with scammers. Each study experienced limitations from a technological, demographic, and geographic angle. While each study was able to present the basic terms of the issue, they were only able to do so at a limited capacity. The studies did not expand on a broader level. The second section was more

background information on the current acts being used as protective measures. Protective measures are limited due to being outdated in the technological world of today. The art of' scambaiting using social media platforms, such as YouTube, is an interesting and effective subgenre for bringing awareness of the scams and even getting a few of the scam call centers shut down. The limitations they have are that these call centers are able to build up rapidly because they front as a legitimate business making it difficult for authorities to locate and shut them down. There is also criticism on the validity of these YouTube scam baiters, people question whether they are legit or not.

The third section of this paper focused on solutions for the future. Based on the research done for this paper, there are still academic gaps in finding future solutions to this issue. One of the reasons for these gaps in literature lies in technology. Technology is constantly changing and evolving at a rapid pace. The use of Artificial Intelligence (AI) could make the problem worse in the future. I agree with Ammirrul and Zukry (2024) on the fact that in the future there needs to be a collaboration between technology developers, policy makers, and financial institutions, as well as community organizations to address safety of the elderly community in the realm of cybersecurity. Having a safer and more inclusive online environment can enhance elements of security and confidence for the elderly community

References

CBS Interactive. (2014). *Evolution of the phone: From the first call to the next frontier*. CBS News. https://www.cbsnews.com/news/evolution-of-the-phone-from-the-first-call-to-the-next-frontier/

Combating spoofed robocalls with caller ID authentication. Federal Communications Commission. (2021). https://www.fcc.gov/call-authentication

Cyphers, B. (2020). *A guided tour of the data Facebook uses to target ads*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2019/01/guided-tour-data-facebook-uses-target-ads

Duran v. La Boom Disco, inc., no. 19-600 (2d Cir. 2020). Justia Law. https://law.justia.com/cases/federal/appellate- courts/ca2/19-600/19-600-2020-04-07.html

Egan, N. (2022). Rage against the machine: Reducing robocall abuse to protect at-risk consumers. *University of Massachusetts Law Review*, *17*(2), 211–235. https://doi.org/https://scholarship.law.umassd.edu/umlr/vol17/iss2/4?utm_source=scholarship.law.umassd.edu%2Fumlr%2Fvol17%2Fiss2%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages

Fowle, D. (2024). *Retired Duluth couple loses life savings to phone scammers*. FOX 5 Atlanta https://www.fox5atlanta.com/news/one-slick-phone-call-and-duluth-couple-lost-life-savings

Hamm, A. (2021). *Facebook Inc. v. Duguid*. SCOTUSblog. https://www.scotusblog.com/case-files/cases/facebook-inc-v-duguid/

Mazzuchetti, L. A. (2021). *Supreme Court defines ATDS under the TCPA*. Kelley Drye & Warren LLP. https://www.kelleydrye.com/viewpoints/blogs/ad-law-access/supreme-court-ruled-that-the-definition-of-an-automatic-telephone-dialing- system-under-the-tcpa-is-limited-by-the-plain-grammar-of-the-statute-itself

National do not call registry data book for fiscal year 2020 | Federal Trade Commission. (n.d.). https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2020

Parti, K., & Tahir, F. (2023). If we don't listen to them, we make them lose more than money: Exploring reasons for underreporting and the needs of older scam victims. *Social Sciences*, *12*(5), 264. https://doi.org/10.3390/socsci12050264

Pitts & Williams. (2021). *Scam robocalls drop 30% with new FCC* News https://www.12news.com/article/news/investigations/robocalls/scam-robocallsdrop-30-with-new-fcc-mandate/75-db058d1e-fbdf-4a89-98d9-9a35d435d4be [https://perma.cc/P5FJ-QFK9]

Price , S. (2021). *Stop the calls: Robocallers Trick grandmother out of life savings. CBS8*. https://www.cbs8.com/article/news/investigation /robocalls/robocalls-featured/stop-the-calls- robocallers-trick-grandmother-out-of-life-savings/509-5c84adac-729e-4b2a-ac54 0be16e1e475a

Robinson, J., & Edwards, M. (2024). Fraudsters target the elderly: Behavioral evidence from randomized controlled scam-baiting experiments. *Security Journal*, 1–24. https://doi.org/10.1057/s41284-023-00410-4

Sonam, J. (2022). *How Four International YouTube Sleuths Teamed Up To Expose Call Centre Scams in Kolkata.* https://timesofindia.indiatimes.com/home/Sunday-times/how-four-international-youtube-sleuths-teamed-up-to-expose-call-centre-scams-in-kolkata/articleshow/91859500.cms

Sherman, Imani and Delgado, Daniel and Gilbert, Juan and Ruiz, Jaime and Traynor, Patrick, Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. (2021). TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, Available at SSRN: https://ssrn.com/abstract=3898127

Ueno, D., Daiku, Y., Eguchi, Y., Iwata, M., Amano, S., Ayani, N., Nakamura, K., Kato, Y., Matsuoka, T., & Narumoto, J. (2021). Mild cognitive decline is a risk factor for scam vulnerability in older adults. *Frontiers in Psychiatry*, *12*, 8.https://doi.org/10.3389/fpsyt.2021.685451

Wagner, K. (2018, April 11). *This is how Facebook uses your data for AD targeting*. Vox. https://www.vox.com/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg

ZUKRY, M. A. A. B. M., & BIN, M. N. A. (2024). Strategies for protecting senior citizens against online banking fraud and scams: A systematic review. *Journal of Theoretical and Applied Information Technology*, *102*(14).https://docs.google.com/document/d/1OMDEZ4pJRE_Z86EcIBomS8CyP4kT8i5eMOHvoWUEzmY/edit?usp=sharing