FIGHTING FRAUD AND SCAMS DURING THE COVID-19 PANDEMIC: REPORTS FROM THE MASSACHUSETTS AGING SERVICES NETWORK

BY ANNA-MARIE TABOR; ELIZBETH DUGAN; AND TAYLOR JANSEN*

* Anna-Marie Tabor is an Assistant Professor at the University of Massachusetts School of Law. Elizabeth Dugan is Associate Professor of Gerontology at the University of Massachusetts Boston. Taylor Jansen is a Postdoctoral Fellow in Gerontology at the University of Massachusetts Boston. The authors wish to express our gratitude to Margaret Drew, Hillary Farber, Jeannine Johnson, and Maria O'Brien for providing feedback on the drafts of this Article. We also wish to thank Amanda Baker for her research assistance, and Emily Kennerley for her help with survey administration. This project was funded by an Academic Research Grant from the Albert and Elaine Borchard Foundation Center on Law and Aging.

ABSTRACT

Older Americans reported losing $5.7 billion to fraud and scams during the COVID-19 pandemic – a number that almost certainly underrepresents the true size of the problem. Agencies serving older adults witnessed in real-time the devastation these scams caused their clients, both financially and psychologically. This Article publishes new research surveying Massachusetts aging services providers about their efforts to address fraud targeted at older people during the pandemic. The results provide a community-based viewpoint on the crisis, shedding new light on the experiences of local providers and the individuals they serve. An overwhelming majority of respondents had learned of a client who fell victim to a financial scam during the pandemic; their narratives conveyed frustration with the vast scope of an issue far exceeding their organizations' limited resources. They described efforts to teach clients how to recognize and avoid scams, yet they also observed how trained participants nonetheless lost money to fraud. They described helping their clients to file police reports, yet they also suggested that law enforcement efforts are not proceeding quickly enough, leaving them to wonder whether reporting may be pointless for many victims. As fraud numbers continue to rise, greater engagement between community aging services providers and other stakeholders – especially law enforcement and financial institutions – will play a critical role in the ongoing fight. A streamlined reporting process would help aging services to connect their clients promptly with law enforcement and financial institutions to reduce money lost, and with counseling and other resources to facilitate financial and emotional recovery. A centralized resource center that provides high-quality, up-to-date, and accessible training materials would ensure that many hundreds of local organizations do not have to reinvent the wheel to educate their clients. While difficult work lies ahead, local aging services providers stand ready to test and deploy emerging strategies, drawing on decades of service to older Americans to address this latest challenge.

INTRODUCTION

In 2021, William and Ave Bortz received what they thought was an important email message from the online retailer Amazon about suspicious activity on their account.[1] They did not realize that this was in fact a phishing attack – a fraudulent email intended to lure them into a costly scam. Over the following week, scammers took remote control of their personal computer and coached them through several large wire transfers to foreign bank accounts. Before their daughter finally intervened, the Bortzes, who were in their mid-70s, transferred funds worth almost $700,000 to the foreign accounts. The money included proceeds from the recent sale of the family home, and the theft left the couple without life savings they had been counting on to support their retirement.

Hundreds of thousands of other older individuals who were scammed during the COVID-19 pandemic shared their own stories with the Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI).[2] In 2022 alone, the IC3 received over 88,000 fraud complaints involving people over the age of 60, with losses totaling $3.1 billion.[3] This dollar amount was 80% greater than the previous record set in 2021.[4]

The sheer volume of money lost represents tremendous hardship to victims and their families. For many older people, the lost funds represent meals forgone, medications skipped, and rent left unpaid. Others lose the nest egg they had been relying on to support themselves through retirement. The FBI's 2022 IC3 data shows that victims over the age of 60 lost on average $35,101, and more than 5400 victims reported losing over $100,000.[5]

Beyond these monetary losses, a scam can have devastating psychological consequences.[6] After learning that they have been victimized, older people may

---

[1] William and Ave Bortz described their ordeal in a complaint filed in the Superior Court for the State of California, County of San Diego, and subsequently removed to the U.S. District Court for the Southern District of California. *See* Bortz v. JPMorgan Chase Bank, NA, 2022 WL 1489832 (S.D. Ca. May 10, 2022). They alleged violations of California's Elder Abuse Law and Unfair Competition Law, and breach of implied covenant of good faith and fair dealing. *Id.* Their complaint was dismissed, and the Ninth Circuit upheld the dismissal on appeal. *See* Bortz v. JP Morgan Chase Bank, (9th Cir 2023) 2023 WL 4700640. Additional details are recounted in Melissa Mecija, *Elderly Couple Loses Nearly $700K Online Scam*, ABC 10 NEWS SAN DIEGO (Aug. 26, 2022, 2:02 AM), https://www.10news.com/news/team-10/elderly-couple-loses-nearly-700k-online-scam [https://perma.cc/F3PZ-D6NZ].

[2] FED. BUREAU OF INVESTIGATION, ELDER FRAUD REPORT 2022 4 (2022), https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf [https://perma.cc/B7M3-935E] [hereinafter "2022 FBI ELDER FRAUD REPORT"].

[3] *Id.*

[4] *Id.* at 4-5.

[5] *Id.* at 4.

[6] *See* FINRA INV. EDUC. FOUND., NONTRADITIONAL COSTS OF FINANCIAL FRAUD: REPORT OF SURVEY FINDINGS 16-18 (2016), https://www.finrafoundation.org/sites/finrafoundation/files/nontraditional-costs-financial-fraud_0_0_0.pdf [https://perma.cc/WA8U-HFUN].

feel hurt, embarrassed, angry, depressed, or anxious.[7] They may lose their confidence to evaluate the legitimacy of communications in other contexts, and may socially withdraw.[8] They may fear losing their independence, especially if family members or others take control of their affairs in response to the incident.[9] These concerns may spiral into further isolation and fearfulness, or even poor health outcomes.[10] What starts as a financial crime may become a vicious cycle affecting long-term well-being.[11]

Throughout the pandemic, the country's network of aging services providers stood witness to these scams and sounded the alarm to their clients, service partners, and communities. Founded by Congress with the passage of the Older Americans Act,[12] the U.S. Aging Services Network includes Area Agencies on Aging, municipal Councils on Aging, and other state and local organizations serving a variety of needs.[13] They provide meals, social engagement programs, caregiver support, and other programs that are critical to the health and well-being of their clients, who primarily are individuals over the age of 60.[14]

---

[7] *See* Yuxi Shang et al., *The Psychology of the Internet Fraud Victimization of Older Adults: A Systematic Review*, 13 FRONTIERS IN PSYCH. 912242 (Sept. 5, 2022).

[8] *See* CONSUMER FIN. PROT. BUREAU, *RECOVERING FROM ELDER FINANCIAL EXPLOITATION: A FRAMEWORK FOR POLICY AND RESEARCH* 1, 40 (2022), https://files.consumerfinance.gov/f/documents/cfpb_recovering-from-elder-financial-exploitation_report_09-2022.pdf [https://perma.cc/8BKH-WXKV] [hereinafter "CFPB FRAMEWORK 2022"].

[9] *See id.* at 25-26.

[10] *See id.* Cognitive decline also has been linked to susceptibility to fraud in older adults. *See* Shang et al., *supra* note 7. An older adult's experience falling victim to a financial fraud may prompt family members to investigate the possibility of dementia or other cognitive impairment. *See* Tianyi Zhang et al., *Elder Financial Exploitation in the Digital Age*, 51(2) J AM. ACAD. PSYCHIATRY L. 1, 3 (2023).

[11] Another pandemic-era incident reported by AARP illustrates how a brief internet exchange can balloon into an emotional crisis. A 75-year-old woman from the Los Angeles area posted a message on Instagram tagging a television journalist she admired. A scammer who saw this public message impersonated the journalist and lured the woman into a complex and costly scam. The scammers accused her of money laundering and demanded that she pay tens of thousands of dollars to avoid prosecution. The woman lost approximately $70,000, became suicidal, and checked herself into a hospital, where a psychiatrist explained to her that she had been scammed. Christina Ianzito, *Many Victims Struggle With Mental Health in Scams' Aftermath*, AARP (Dec. 15, 2022) https://www.aarp.org/money/scams-fraud/info-2022/mental-health-impact.html [https://perma.cc/QQ3C-PKRW].

[12] Older Americans Act of 1965, Pub. L. No. 89-73, § 3021 et seq. (codified at 42 U.S.C. § 3001-3045).

[13] *See* Aging and Disability Networks, ADMIN. FOR CMTY. LIVING, https://acl.gov/programs/aging-and-disability-networks [https://perma.cc/ST3U-9QUE] (last modified on Sept. 9, 2024) (describing the various government agencies and other organizations that make up the national Aging Services Network).

[14] *See* NAT'L ASS'N OF AREA AGENCIES ON AGING, #AAAS AT WORK FOR OLDER ADULTS: A SNAPSHOT OF AREA AGENCY ON AGING RESPONSES TO COVID-19 1, 4 (2020), https://www.usaging.org/Files/n4a_MemberSurveyReport2020_Web_07July2020.pdf

These agencies adjusted to COVID health threats and social distancing requirements by transitioning to remote service modalities.[15] In many cases, they dramatically transformed programs, adopting new, virtual technologies, and increasing the use of telephonic services.[16] They also gained first-hand knowledge of the challenges facing their clients during the period, including the rise in fraud.[17] They became, by default, first responders to scams, on top of the many other new challenges and responsibilities that they assumed due to COVID.[18]

This Article examines the role of aging services organizations in responding to fraud and scams during the pandemic, reporting the results of a survey of agencies in Massachusetts that serve people over the age of 60. Almost all survey respondents knew of clients who had encountered fraud or scams during the pandemic. Their responses indicated that they were engaged with clients to help them avoid fraud and to assist in reporting incidents. Yet they also expressed their frustration with the challenges of navigating a complex and decentralized anti-fraud system. While they diligently sounded the alarm, they also harbored doubts about whether their message was heard by either their clients or other anti-fraud stakeholders.

Section I of this Article provides a brief overview of fraud and scams against older people, including an explanation of the terminology used and an examination of trends during the COVID pandemic. Section II describes the U.S. Aging Services Network and the many ways that its organizations enhance quality of life for older Americans. The terms "aging services organization" and "aging services provider" as used in this Article include private and public entities that offer a variety of social services, primarily to people over the age of 60.[19] The survey described in this Article included senior centers, Area Agencies on Aging, Aging Services Access Points, and legal services organizations that help older people.[20]

The Article next turns in Section III to the survey conducted by the authors in 2022 to learn how aging services organizations in Massachusetts experienced fraud and scams during the pandemic. The results provide insight regarding best practices during the COVID crisis and the role that these organizations can play in fighting fraud in the future. On the basis of the survey results, Section IV recommends more effective and streamlined integration of local community

[https://perma.cc/64K2-67LR] [hereinafter #AAAs AT WORK]. Since this network was founded, the need for its services has grown as the number of older Americans has increased. Haley B. Gallo & Kathleen H. Wilber, *Transforming Aging Services: Area Agencies on Aging and the COVID-19 Response*, 61 Gerontologist 152, 154 (2021).

[15] *See* #AAAs AT WORK, *supra* note 14, at 4, 11.

[16] See *id.*

[17] *See infra* Section II.

[18] *See infra* Section II.

[19] *See infra* Section II.

[20] *See infra* Section III.

efforts with efforts of other stakeholders, including both financial institutions and state and national law enforcement. Aging services providers will be better equipped to help their clients avoid, recognize, and recover from fraud and scams if they are notified about the latest developments in prevention and enforcement, and if they have access to the most up-to-date information to share with their clients. Banks and enforcement agencies will benefit if they leverage the unique expertise of community-based organizations regarding the needs of the older people. The Article also recommends a streamlined incident reporting system and centrally-created educational and training resources.

I. AN OVERVIEW OF FRAUD AND SCAMS DURING THE COVID-19 PANDEMIC

A. *Defining Elder Financial Exploitation*

"Elder financial exploitation"[21] is an umbrella term commonly defined as "illegal or improper use of an older adult's funds, property, or assets."[22] Within this larger category, policy makers and scholars typically distinguish these financial crimes by whether the victim knows or does not know the perpetrator.[23] When the victim knows the perpetrator, or the perpetrator is otherwise abusing a position of trust, the activity is typically referred to as "financial abuse."[24] If

[21] "Older adults" is used to refer to adults aged 60 and over. This is the definition of "older individuals" in the Older Americans Act of 1965, which created the Aging Services Network. Older Americans Act of 1965, Pub. L. No. 89-73, § 102 (40) (codified at 42 U.S.C. § 3001-3045). In recent years, the use of the term "older adults" has become preferred over "elders" in many contexts, although the term "elder" also continues in use. This Article uses the term "older adults" except where the use of the term "elder" is necessary for accuracy or clarity. For a description of the changing language of aging, *see* Robert Weisman, *Who Are You Calling Senior? For Older Folks, Some Terms Are Fast Becoming Radioactive*, BOS. GLOBE (Mar. 7, 2019), https://www.bostonglobe.com/metro/2019/03/07/who-are-you-calling-senior-for-older-folks-some-terms-are-fast-becoming-radioactive/EaCvwK6WJIHbtcoXO63JqO/story.html [https://perma.cc/WQB7-4J6T].

[22] Stephen Deane, ELDER FINANCIAL EXPLOITATION: WHY IT IS A CONCERN, WHAT REGULATORS ARE DOING ABOUT IT, AND LOOKING AHEAD, U.S. SEC. AND EXCH. COMM'N OFF. OF THE INV. ADVOC. 1 (June 2018), https://www.sec.gov/files/elder-financial-exploitation.pdf [https://perma.cc/XHG3-Y6QZ] [hereinafter "SEC ELDER FINANCIAL EXPLOITATION REPORT"] (quoting U.S. GOV'T ACCOUNTABILITY OFF., GAO 11-208, ELDER JUSTICE: STRONGER FEDERAL LEADERSHIP COULD ENHANCE NATIONAL RESPONSE TO ELDER ABUSE, 4 (2011)).

[23] Marguerite DeLiema, *Elder Fraud and Financial Exploitation: Application of Routine Activity Theory*, 58 GERONTOLOGIST 706, 707 (2016) [hereinafter DeLiema, *Elder Fraud and Financial Exploitation*].

[24] Financial abuse is one of several types of elder abuse, which is defined by the U.S. Centers of Disease Control as "an intentional act or failure to act that causes or creates a risk of harm to an older adult . . . often [] at the hands of a caregiver or a person the elder trusts." Nat'l Ctr. for Inj. Prevention and Control, *Preventing Elder Abuse*, U.S. CTR. FOR DISEASE CONTROL (2020), https://www.cdc.gov/violenceprevention/pdf/elder/.

the victim does not know the perpetrator, then "financial fraud" is the appropriate term.[25] In this Article, we follow the example of several U.S. government agencies and use the term "fraud and scams" to refer to exploitation by a stranger, which is our focus.[26]

The scourge of fraud and scams committed by strangers devastates millions of lives each year.[27] Like William and Ave Bortz, many victims lose large amounts of money, resulting in significant harm to their financial security.[28] Yet relatively smaller monetary losses can also create a financial hardship, particularly for lower-income people who may already be struggling to afford basic necessities.

The psychological impacts are also devastating. Victims often do not appreciate that scams are widespread, sophisticated, and highly effective, instead concluding that falling for a scam is a personal failing and cause for embarrassment and shame.[29] This is illustrated by the results of a 2015 survey of fraud victims in which 47% of participants reported that they agreed with the

EA_Factsheet.pdf [https://perma.cc/WM6A-JPXF]. Other types of elder abuse include physical abuse, sexual abuse, emotional or psychological abuse, and neglect, in addition to financial abuse. *Id.*; *see also* U.S. GOV'T ACCOUNTABILITY OFF., GAO 11 208 4, ELDER JUSTICE: STRONGER FEDERAL LEADERSHIP COULD ENHANCE NATIONAL RESPONSE TO ELDER ABUSE (2011).

[25] *Id.*

[26] *See, e.g.*, CFPB FRAMEWORK 2022, *supra* note 8 (which uses the terms "fraud" and "scams" throughout; *Elder Justice Initiative*, DEP'T OF JUST. https://www.justice.gov/elderjustice [https://perma.cc/SF48-NYZQ] (last visited Oct. 25, 2023) (stating that the mission of the Elder Justice Initiative is "to support and coordinate the Department's enforcement and programmatic efforts to combat elder abuse, neglect and financial fraud and scams that target our nation's older adults"); Patrick J. Kiger & Sari Harrar, *6 Top Scams to Watch Out for in 2024*, AARP (Dec.. 20, 2023), https://www.aarp.org/money/scams-fraud/info-2023/top-scammer-tactics-2023.html?intcmp=AE-FRDSC-MOR-R2-POS3 [https://perma.cc/HVJ4-R54L]. In some contexts, a "scam" may be differentiated from a "fraud" by whether the victim is misled into revealing their personal information or is otherwise directly involved in the original breach. For example, according to this usage, a scheme in which an account is accessed using data stolen in a large security breach would be categorized as a fraud; but if the account owner is tricked into sharing a passcode, then the scheme would be categorized as a scam. *See, e.g.*, Dawn Kellogg, *Fraud and Scams – There's a Big Difference*, THE SUMMIT FED. CREDIT UNION: THE SUMMIT BLOG (Nov. 15, 2023), https://www.summitfcu.org/blog/fraud-and-scams-theres-a-big-difference/ [https://perma.cc/M5XG-MVNT].

[27] Zhang et al., *supra* note 10, at 1.

[28] As described above, in 2022, more than 5400 victims reported to the FBI that they lost more than $100,000. *See* 2022 FBI ELDER FRAUD REPORT, *supra* note 2 and accompanying text.

[29] *See* CFPB FRAMEWORK 2022, *supra* note 8, at 25-26 (noting that "older adults often fear loss of independence following [elder financial exploitation], which may be heightened if they are in the early stages of cognitive decline").

statement, "I blame myself for being defrauded."[30] Physical well-being also can suffer, particularly if the incident results in greater isolation and reduced independence for the victims.[31]

B. *Measuring the Extent of the Problem*

Millions of Americans lost billions of dollars to fraud during the COVID-19 pandemic, with incidents exploding across all age cohorts.[32] The Federal Trade Commission (FTC) reported that in 2022 alone, consumers of all ages filed 2.4 million fraud reports through its Consumer Sentinel database.[33] Reported losses in 2022 totaled $8.8 billion.[34]

Incidents involving older people were a significant component of this increase in fraud overall. Reports to the FBI's IC3 involving fraud against people over 60 jumped by almost 30% between 2019 and 2022.[35] The dollar amount lost by victims in this age group was a staggering $5.7 billion for the three-year period spanning 2020 to 2022.[36] Reported losses increased each year during the

[30] *See* FINRA, *supra* note 6, at 13.

[31] *See* Zhang et al., *supra* note 10, at 1.

[32] The FBI's annual Internet Crime Reports publish the numbers of reported incidents by age cohort, and demonstrate how reports increased during the pandemic across all age cohorts. *Compare* FED. BUREAU OF INVESTIGATION, 2019 INTERNET CRIME REPORT, INTERNET CRIME COMPLAINT CTR. 3, 16, (2019), https://www.ic3.gov/Media/PDF/AnnualReport /2019_IC3Report.pdf, *with* FED. BUREAU OF INVESTIGATION, 2022 INTERNET CRIME REPORT, INTERNET CRIME COMPLAINT CTR. 3, 16, (2022), https://www.ic3.gov/Media /PDF/AnnualReport/2022_IC3Report.pdf.

[33] Press Release, Fed. Trade Comm'n, New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022 (Feb. 23, 2023), https://www.ftc.gov/news-events/news /press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022 [https://perma.cc/2J7U-UMXV].

[34] *Id.* Total losses reported to the FBI during the period 2020-2022 were reported at $21.4 billion. The number of complaints to the FBI jumped 69% between 2019 and 2020, and an additional 7% from 2020 to 2021. There was a small decrease in number reports to the FBI from 2021 to 2022. The total number of reports in 2021 was 847,376, and the number in 2022 was 5.5% lower, at 800,944. *See* FBI INTERNET CRIME REPORT 2022, *supra* note 32.

[35] In 2019, there were 68,013 reports involving people over the age of 60, and $835,164,766 in reported losses. *See* FED. BUREAU OF INVESTIGATION, 2019 INTERNET CRIME REPORT, INTERNET CRIME COMPLAINT, *supra* note 32. In 2022, there were 88,262 reports involving people over the age of 60, and $3.1 billion in reported losses. FBI INTERNET CRIME REPORT 2022, *supra* note 32, at 18.

[36] *See infra* note 37.

pandemic, reaching $3.1 billion in 2022.[37] This represented an extraordinary 82% increase over the losses from 2021 in the over 60 cohort.[38]

Although this Article focuses on older people and fraud, it is important to note that fraud negatively impacts adults of all ages. In fact, several studies have indicated that younger cohorts may be more likely than older adults to lose money to scams.[39] People aged 30-39 make the greatest number of fraud and scam reports to the FBI and FTC, although dollar losses are highest for people

[37] In 2020, the FBI reported $966 million in losses to people over 60; in 2021, $1.7 billion; and in 2022, $3.1 billion. *See* FED. BUREAU OF INVESTIGATION, 2020 ELDER FRAUD REPORT, INTERNET CRIME COMPLAINT CTR. 4 (2020), https://www.ic3.gov/AnnualReport/Reports/2020_IC3ElderFraudReport.pdf [https://perma.cc/623C-VC7M];
FED. BUREAU OF INVESTIGATION, 2021 ELDER FRAUD REPORT 4 (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf [https://perma.cc/4MC3-RT2V]; 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 4.

[38] FED. BUREAU OF INVESTIGATION, 2022 INTERNET CRIME REPORT, *supra* note 32, at 4. Another source of data on fraud is provided by Suspicious Activity Reports (SARs) that are mandated by the Bank Secrecy Act of 1970, an anti-money laundering statute. Bank Secrecy Act of 1970, Pub. L. No. 91-508 (1970). Financial institutions that learn of fraud or suspected fraud are required to file a SAR describing the suspected criminal activity so that regulators and law enforcement may follow up as required. Institutions transmit the SARs to the Financial Crimes Enforcement Network (FinCEN), which is a component of the U.S. Treasury Department. The CFPB reports that over 62,000 elder financial exploitation SARs were filed in 2020 alone. RECOMMENDATIONS AND REPORT FOR FINANCIAL INSTITUTIONS ON PREVENTING AND RESPONDING TO ELDER FINANCIAL EXPLOITATION, CONSUMER FIN. PROT. BUREAU 3, 16 (2016), https://files.consumerfinance.gov/f/201603_cfpb_recommendations-and-report-for-financial-institutions-on-preventing-and-responding-to-elder-financial-exploitation.pdf [https://perma.cc/Q7CH-G92C].

[39] Yaniv Hanoch & Stacey Wood, *The Scams Among Us: Who Falls Prey and Why*, 30(3) CURRENT DIRECTIONS IN PSYCH. SCI., 260, 261 (2021) ("[C]urrent data do not provide a clear picture about the relationship between age and susceptibility to scams, and there is little insight as to why middle-aged adults are at particularly high risk."). A survey conducted in 2017 and 2018 found that "[o]n average, those who lost money were 2-3 years younger than those who were targeted for a scam but did not engage." *See* Marti DeLiema et al., *Exposed to Scams: What Separates Victims From Non-Victims?*, FINRA INVEST. EDUC. FOUND. 7 (2019), https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-what-separates-victims-from-non-victims_0_0.pdf [https://perma.cc/SJ6J-AN7G] [hereinafter DeLiema et al., *Exposed to Scams*]. *See also* James Toomey, *The Age of Fraud*, 60 HARV. J. ON LEGIS. 101, 101 (2023) (revealing that a survey conducted in 2020 found that younger people were more likely to engage with scams than were older people).

over 60.[40] Section I.D of this Article explores several possible reasons why fraud against older people in particular increased during the pandemic.[41]

The enormous volume of complaints almost certainly understates the true scope of the problem. Experts widely acknowledge that victims significantly underreport financial scams and other financial exploitation.[42] As noted previously, individuals who experience these scams often feel shame and embarrassment, making them reluctant to share their experiences with others by reporting.[43] Many people believe that reporting is a waste of time because lost funds are seldom recovered.[44] Among older victims, physical and cognitive impairment may pose additional barriers to reporting.[45]

Furthermore, victims who wish to file a report face a decentralized reporting infrastructure consisting of a bewildering array of federal and state enforcement and social service agencies.[46] At the federal level, reporting options include the US DOJ's National Elder Fraud Hotline for crimes against older people; the FBI's IC3 for internet-related crimes; and the FTC's Consumer Sentinel Database, among others. Rather than reporting to these federal authorities,

[40] FED. BUREAU OF INVESTIGATION, 2022 INTERNET CRIME REPORT, *supra* note 32, at 18; *Who experiences scams? A story for all ages*, FED. TRADE COMM'N: DATA SPOTLIGHT (2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages [https://perma.cc/YFL7-VWZD] [hereinafter "FTC DATA SPOTLIGHT 2022"].

[41] In a recent article, James Toomey advocates for greater focus on how fraud impacts younger people. *See* Toomey, *supra* note 39, at 105 (reporting results of survey conducted in 2020 that found that younger people were more likely to engage with scams than were older people). Efforts to fight the fraud epidemic will be most effective if they can be tailored to different groups – including different age groups – based on risk factors, frames of mind and preferred methods and styles of communication. *See* CRAIG HONICK ET AL., EXPOSED TO SCAMS: CAN CHALLENGING CONSUMERS' BELIEFS PROTECT THEM FROM FRAUD? 26 (FINRA Inv. Educ. Found. 2021), https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-can-challenging-consumers-beliefs-protect-them-from-fraud.pdf [https://perma.cc/A79Y-V8P3].

[42] *See* CFPB FRAMEWORK 2022, *supra* note 8, at 19 (citing Mark Lachs & Jacquelin Berman, *Under the Radar: New York State Elder Abuse Prevalence Study*, N.Y. STATE OFF. OF CHILD. AND FAM. SERV. (2011)).

[43] *See* CFPB FRAMEWORK 2022, *supra* note 8, at 22. One individual who was interviewed by the CFPB for its report described his reluctance to file a complaint after losing money in an investment scam. He shared that he "did not involve law enforcement because [he was] just taking responsibility for [his] own decision . . . to put money into something that [he] shouldn't have.'" *Id.*

[44] *See id.* at 24. For example, some victims believe that law enforcement will not bother to investigate incidents, or that law enforcement simply is incapable of tracing scams to recover lost funds. *See id.* While unfortunately the large majority of fraud incidents reported to law enforcement are never resolved, the likelihood of recovering funds is virtually nonexistent when incidents go unreported. *See id.* at 19.

[45] *See id.* at 24–25.

[46] *See id.* at 25.

victims may turn to their state or local police departments. Or they may contact non-law enforcement helplines, such as the AARP's Fraud Watch Network Helpline.[47] While some reporting centers share data with each other, not all do, or their data sharing may be incomplete.[48]

Despite these data limitations, there is widespread agreement that fraud and scams increased dramatically during the pandemic years. The upward trend has continued since the survey was distributed in 2022, suggesting that this is an entrenched problem that will continue to harm older adults in the years to come. In 2023, the FBI IC3 reported increases in both reports and losses by people over 60 from the prior year,[49] while the FTC's Consumer Sentinel Database reported an increase of 20% in total losses recorded.[50] According to the IC3, $3.4 billion was reported stolen from older adults in 2023.[51]

C. *Varieties of Scams*

Scammers use a broad and expanding variety of deceptions, with the FBI's IC3 categorizing reports into more than two dozen separate types of scams.[52] While specific methods and strategies are constantly evolving, the following list describes several common types.

Tech Support Scams. In a tech support scam, someone posing as a technical expert contacts the victim and convinces them either to pay for technical support services that they do not need or to grant access to personal or financial information that can then be used to steal their assets or identity.[53] These were

[47] The AARP provides a free Fraud Watch Network Helpline to counsel and advise callers who have encountered scams. *See* Christina Ianzito, *How AARP's Fraud Watch Network Helpline Is Fighting for You*, AARP (May 3, 2023), https://www.aarp.org/money/scams-fraud/info-2023/helpline-volunteers.html [https://perma.cc/9CNP-A5SK].

[48] *See* PROTECTING OLDER CONSUMERS 2022-2023, FED. TRADE COMM'N 39 (2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf [https://perma.cc/J7N7-X6M2].

[49] *Federal Bureau of Investigation Elder Fraud Report 2023*, INTERNET CRIME CTR. 5 (2022), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf [https://perma.cc/8LHK-AD74] [hereinafter "2023 FBI ELDER FRAUD REPORT"].

[50] *See* FEDERAL TRADE COMMISSION FRAUD REPORTS, TABLEAU PUB., https://public.tableau.com/app/profile/federal.trade.commission/vizzes (select "Fraud Reports" then "Age & Fraud," then change the selected year to 2022 and to 2023).

[51] 2023 FBI ELDER FRAUD REPORT, *supra* note 49, at 3.

[52] See 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 8. There are variations in the categories and definitions used across agencies; for example, the FTC's reporting on fraud against older Americans counts "Romance Scams" and "Family and Friend Imposters" as two separate categories of scams, while the FBI's IC3 report combines them into a single category, "Confidence/Romance Scams." *See id.*; FED. TRADE COMM'N, PROTECTING OLDER CONSUMER 2022-2023 31 (2023).

[53] *See id.* at 12, 18; ADVISORY ON ELDER FINANCIAL EXPLOITATION, FIN. CRIME ENF'T NETWORK 7 (June 15, 2022), https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%

by far the most frequent type of scam reported to the FBI in 2022 involving people over the age of 60, resulting in $587 million in losses that year.[54]

Investment Scams. Investment scams use the guise of legitimate and potentially lucrative financial opportunities to steal large sums.[55] This category of scam was the costliest in 2022 for people over 60, resulting in losses worth over $990 million.[56] The FBI reports that older victims are uniquely vulnerable to investment scams if they are convinced to turn over their retirement account balances or the equity in their homes.[57]

Non-payment/Non-delivery Scams. This category includes scams where the victim pays for goods or services that are never provided, and scams where the victim provides goods or services to the perpetrator but never is paid.[58] In 2022 these were the second most frequently reported scam to the FBI's IC3 involving people over 60, at 7,985 reports, and over $51 million lost.[59]

Confidence/Romance Scams. These include scams in which someone uses a false identity to convince the victim that a close relationship exists between them and then uses that trust to steal from the victim.[60] In addition to romance scams, the "Grandparent Scam," in which someone impersonates a relative, such as a grandchild, also falls within the category of confidence scams.[61] Confidence and romance scams resulted in $419 million in reported losses in 2022 to people over 60.[62]

"Pig Butchering" is a variety of confidence scam in which a scammer assumes a false identity and then gradually develops a relationship with the victim, "fattens" the victim, and eventually "butchers" them by convincing them to transfer large sums of money to the scammer.[63] The scam generally begins with a private message sent via social media that appears to the recipient as though it was innocently sent in error to the wrong account.[64] If the target responds, the scammer works to develop a relationship and build trust before conning the target into transferring money to a fake account, generally under the auspices of

20508.pdf [https://perma.cc/S2GM-7H8E] [hereinafter "2022 FINCEN ADVISORY ON ELDER EXPLOITATION"].

[54] In 2022, the FBI received 17,810 reports concerning tech support scams involving people over 60. 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 6-7.

[55] *See id.* at 13.

[56] *Id.* at 7.

[57] *See id.* at 13.

[58] *See id.* at 18.

[59] *Id.* at 6-7.

[60] *See* 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 14.

[61] *See id.* at 14.

[62] *Id.* at 7.

[63] *See* Cezary Podkul, *What's a Pig Butchering Scam? Here's How to Avoid Falling Victim to One*, PROPUBLICA (Sept. 29, 2022), https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one [https://perma.cc/873X-L9SH].

[64] *See id.*

funding a fake investment opportunity.[65] When the victim either runs out of money or realizes that the interaction is fraudulent, the scammer cuts off contact – often after taunting the victim in a manner calculated to discourage them from seeking help from family or law enforcement.[66]

Phishing Scams. Phishing scams involve a communication – usually email, text, or phone call – that impersonates a legitimate entity, but in fact is seeking personal information so that it can be used to steal from the victim.[67] These scams were responsible for $14 million in losses reported to the FBI's IC3 in 2022 to people over 60.[68]

Government Impersonation Scams. These involve the impersonation of officials working for government agencies. In 2022, the FBI's IC3 logged 3,425 reports of such scams and $136 million in losses among people over 60.[69] Scammers may induce cooperation by threatening civil or criminal legal action, such as seizure of bank accounts or arrest.[70]

Lottery/Sweepstakes/Inheritance Scams. In a lottery/sweepstakes scam, the target receives a communication informing them that they won a contest and must pay money up front to claim their prize.[71] Inheritance scams are similar, but the communication purports to relate to a previously-unknown inheritance.[72] People over 60 reported losing $69 million through these types of scams in 2022.[73]

This Article does not focus on frauds that use artificial intelligence ("AI") to trick unsuspecting victims, as such scams had not yet become common during the pandemic years.[74] It is important to note, however, that as this article goes to publication, scammers have begun to use these technologies to create

[65] *See id.*

[66] *See id.*

[67] *See* 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 18.

[68] *Id.* at 7.

[69] *Id.* at 6-7, 17.

[70] *See* 2022 FINCEN ADVISORY ON ELDER EXPLOITATION, *supra* note 53, at 6. The FBI notes that these types of frauds may continue for longer than others because victims may continue to believe that they are in contact with a legitimate government agency for some time before they realize that they have been scammed. *See* 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 12.

[71] 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 13.

[72] *Id.*

[73] *Id.* at 7.

[74] *See* Emily Flitter & Stacy Cowley, *Voice Deepfakes Are Coming for Your Bank Balance*, N.Y. TIMES (Aug. 30, 2023), https://www.nytimes.com/2023/08/30/business /voice-deepfakes-bank-scams.html [https://perma.cc/SGM5-PFN6] (describing in August 2023 how deepfakes only became common within the prior year). While most of the scams reported in the survey did not apparently use AI, one involved a recording of the local senior center director's voice that was fraudulently re-used by scammers to lend legitimacy to their communications. *See infra* text accompanying notes 147-48.

compelling and effective fraudulent campaigns.[75] Sophisticated, AI-driven analytics can sift through extensive stolen data on potential targets and identify those who are most likely to yield the greatest returns.[76] Convincing "deepfakes" of a target's loved one or a trusted public figure can be created using voice and video samples captured through public material on the internet.[77] As AI continues advancing as a preferred criminal tool, innocent consumers will find it increasingly challenging to distinguish between legitimate and illegitimate communications.[78]

D. *Using Routine Activity Theory to Explain Fraud During COVID*

A full explanation of the causes for the dramatic increase in fraud during the pandemic would exceed the scope of this Article, but this section will attempt to contextualize the trends through a leading theoretical approach, Routine Activity Theory. Routine Activity Theory attempts to explain patterns of criminal activity by focusing on the convergence of (1) motivated offenders, (2) suitable targets, and (3) an absence of capable guardianship.[79] First developed by Lawrence E. Cohen and Marcus Felson in 1979, the theory situates criminal activity within the context of the day-to-day activities of victims and offenders, and the circumstances that bring them together.[80] By focusing on the convergence of these three factors, the theory posits that crime rates may change due simply to where victims and offenders are located physically and temporally, and independent of structural changes that also impact them as individuals.[81]

As an approach that developed before widespread internet use, Routine Activity Theory historically was applied in non-virtual settings, where "convergence" referred to the literal meeting in physical space and time of a

[75] *See Modern Scams: How Scammers Are Using Artificial Intelligence & How We Can Fight Back: Hearing Before the Senate Special Committee on Aging*, 118th Cong. (2023) (statement of Tom Romanoff, Director of the Technology Project, Bipartisan Policy Center) (observing that "[g]enerative AI's capacity has gotten so good that most people cannot tell the difference between computer-generated content and human-generated content").

[76] *See id.* (describing how AI-driven automation of confidence and other types of "traditional" scams allows criminals to target more potential victims with greater efficiency).

[77] *See id.*; *see also* Flitter & Cowley, *supra* note 74 ("[T]he speed of technological development, the falling costs of generative artificial intelligence programs and the wide availability of recordings of people's voices on the internet have created the perfect conditions for voice-related A.I. scams.").

[78] *See* Flitter & Cowley, *supra* note 74 (describing efforts to bolster security against deepfakes as "an arms race between the attackers and defenders").

[79] *See* Lawrence E. Cohen & Marcus Felson, *Social Change and Crime Rate Trends: A Routine Activity Approach*, 44 AM. SOCIO. REV. 588, 588 (1979); *see also* Robert J. Bursik, Jr. & Harold G. Grasmick, NEIGHBORHOODS AND CRIME: THE DIMENSIONS OF EFFECTIVE COMMUNITY CONTROL 68-69 (1993).

[80] *See* Cohen & Felson, *supra* note 79, at 589.

[81] *See id.*

motivated offender and suitable target.[82] More recently, researchers have used the theory to help analyze how trends in internet usage impact the prevalence of fraud.[83] Cybercrime brings together victims and offenders from far-flung locations in a largely unregulated forum.[84] Unlike a robbery on a city street, there generally are no eyewitnesses to internet fraud, and there may be little or no opportunity for friends, family, or law enforcement to intervene while the crime is in progress.[85]

Routine Activity Theory also has proven useful in analyzing trends in financial exploitation of older people, including internet-based fraud.[86] While fraud victims include adults of all ages, there are a number of reasons why older people may be "suitable" as targets. Researchers have found, for example, that social isolation increases fraud risk, as can poor physical health.[87] Age-related cognitive impairment is strongly correlated with fraud victimization, due to the impact on the ability to identify a transaction as a scam.[88] Furthermore, even in the absence of cognitive impairment, more typical age-related cognitive changes

[82] *See id.* ("[T]his analysis is confined to those predatory violations involving direct physical contact between at least one offender and at least one person or object which the offender attempts to take or damage."); *see also* Bursik & Grasmick, *supra* note 79, at 68.

[83] *See, e.g.*, Matthew L. Williams, *Guardians upon High: An Application of Routine Activities Theory to Online Identify Theft in Europe at the Country and Individual Level*, 56 BRIT. J. CRIMINOLOGY 21, 23 (2016); Alex Kigerl, *Routine Activity Theory and Malware, Fraud, and Spam at the National Level*, 76 CRIME L. AND SOC. CHANGE 109, 109 (2021).

[84] *But see* Williams, *supra* note 83, at 22, 34 (finding that measures such as anti-virus software and secure browsing are negatively associated with online identify theft).

[85] *See* CFPB FRAMEWORK 2022, *supra* note 8, at 8-9.

[86] See DeLiema, *Elder Fraud and Financial Exploitation*, supra note 23, at 707; *see also* Katalin Parti, *What Is a Capable Guardian to Older Fraud Victims? Comparison of Younger and Older Victims' Characteristics of Online Fraud Utilizing Routine Activity Theory*, 14 FRONTIERS PSYCH., 1, 3 (June 6, 2023).

[87] *See* Marguerite DeLiema et al., *Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type*, 47 INT'L J. OF CONSUMER STUD. 1042, 1054 (2023). Engaging with a scammer is more likely "if [the target does] not have anyone to discuss the offer with," while being unmarried, widowed, or divorced raises the likelihood of losing money. DeLiema et al., *Exposed to Scams*, *supra* note 39, at 7.

[88] *See* Rebecca A. Judges, *The Role of Cognition, Personality, and Trust in Fraud Victimization in Older Adults*, 8 FRONTIERS PSYCH. 1, 6 (2017); *see also* David Brancaccio, *Age of Fraud: Are Seniors More Vulnerable to Financial Scams?*, MARKETPLACE (May 16, 2019), https://www.marketplace.org/2019/05/16/brains-losses-aging-fraud-financial-scams-seniors/ [https://perma.cc/Q9SQ-NCH8]. According to one study, 10% of people over the age of 65 have dementia, and 22% have mild cognitive impairment. *See* Jennifer J. Manly et al., *Estimating the Prevalence of Dementia and Mild Cognitive Impairment in the US*, 79 JAMA NEUROLOGY 1242, 1245 (2022). The prevalence of dementia increases with age, however, with only 3% of participants between the ages of 60 and 69 having dementia; moreover, the percentages were 18% for participants between the ages of 80 and 84, and 35% for participants who were over the age of 90. *Id.* at 1247.

may negatively impact the ability to avoid fraud.[89] Poor physical or cognitive health also can lead an older adult to place greater trust in others by necessity of the circumstances, which could in turn place their financial assets at risk.[90]

As researchers observed a dramatic increase in fraud during the pandemic, they turned to Routine Activity Theory to analyze the growing problem.[91] COVID dramatically disrupted the daily activities of living, including the circumstances under which people worked, socialized, and shopped. Stay-at-home orders significantly restricted interactions outside of the household.[92] After these initial orders were lifted, the U.S. experienced a lengthy period of gradual reopening, when indoor public gatherings remained limited.[93]

Due to their elevated risk for severe COVID-19, many people over the age of 60 continued to voluntarily reduce their social activities, even once vaccines became available.[94] For some, loneliness may have placed them into a mindset where they became overly trusting of strangers, while fewer interactions with family and friends also reduced opportunities to discuss suspicious communications with trusted individuals who could intervene.[95] Technology served as a lifeline to many older people who were physically isolated and relied

[89] *See* Sumit Agarwal, *The Age of Reason: Financial Decisions over the Life Cycle and Implications for Regulation*, *in* BROOKINGS PAPERS ON ECONOMIC ACTIVITY 52, 55-56 (2009). Researchers have found that older people are more likely than younger people to erroneously judge untrustworthy expressions—such as "averted eyes, insincere smiles and a backward tilt of the head"—as trustworthy. *See* Meghan Mott, *Brain Changes as Trust Rises with Age*, NIH RSCH. MATTERS (2012), https://www.nih.gov/news-events/nih-research-matters /brain-changes-trust-rises-age [https://perma.cc/E2H9-CJWK].

[90] 2022 FINCEN ADVISORY ON ELDER EXPLOITATION, *supra* note 53, at 3-4.

[91] *See, e.g.*, Jacky Cheuk Lap Siu et al., *Exploring the Impact of Routine Activity and Financial Strain on Fraud Victimization During the COVID-19 Pandemic in Hong Kong*, 19 ASIAN J. CRIMINOLOGY 441, 441 (2023); Shane D. Johnson & Manja Nikolovska, The Effect of COVID-19 Restrictions on Routine Activities and Online Crime, 40 J. QUANTITATIVE CRIMINOLOGY 131, 131 (2022); Yun Zhang et al., *Vulnerability and fraud: evidence from the COVID-19 pandemic*, 9 HUMAN. AND SOC. SCI. COMMC'NS 424 (2022).

[92] *See* Senan Ebrahim et al., *Reduction of COVID-19 Incidence and Nonpharmacologic Interventions: Analysis Using a US County–Level Policy Data Set*, 22 J. MED INTERNET RSCH. 1 (Dec. 20, 2020) (describing variability of county-level restrictions across the United States instituted in 2020).

[93] *See* Alaa Elassar, *This Is Where Each State Is During Its Phased Reopening*, CNN (May 27, 2020), https://www.cnn.com/interactive/2020/us/states-reopen-coronavirus-trnd/ [https://perma.cc/4AZW-9JQS].

[94] *See* Susan M. Benbow et al., *Invisible and at-Risk: Older Adults During the COVID-19 Pandemic*, 34 J. ELDER ABUSE & NEGLECT 70, 70 (2022); Ellen McCarthy, *The Masked Outliers*, WASH. POST, Oct. 27, 2022, at C1. COVID vaccine administration to health care workers and older people living in long-term care facilities began at the end of 2020, and the vaccine became more widely available over the following months. *See CDC Museum COVID-19 Timeline*, U.S. CTR. FOR DISEASE CONTROL (Mar. 15, 2023), https://www.cdc.gov/museum /timeline/covid19.html [https://perma.cc/7V9S-ZVC7].

[95] *See* DeLiema et al., *Exposed to Scams*, *supra* note 39, at 715.

on remote interactions for everything from medical appointments to social gatherings.[96] As described *infra*, aging services organizations provided their programs remotely as well.[97] Yet, as older adults increased their internet usage, they also raised the likelihood that they would converge with scammers online.[98]

Meanwhile, across the United States and the world, social disruption also pushed organized crime into these same digital spaces.[99] Many offenses against U.S. residents originated at large scam mills in Southeast Asia that are run by criminal syndicates.[100] These international cyber fraud activities scaled dramatically during the pandemic, with a report by the United Nations Office on Drugs and Crime tying the growth to a dearth of other income streams during the period.[101] Scam mill workers are themselves often victims of human trafficking, having been induced to travel to the region by the promise that they would be employed in legitimate technology jobs or call centers.[102] They instead find themselves imprisoned on large, armed compounds, cut off from their

[96] *See* Benbow, *supra* note 94, at 72 ("The inevitable increased use of technology by older adults during lockdowns and social distancing may have exacerbated financial abuse associated with cybercrime, whilst simultaneously attempts to provide equitable, safe access to treatment using virtual health care have imposed new and inadvertent risks of abuse. Although innovative in terms of access, time, and cost effectiveness, virtual/remote care has come with a cost with regards to risk assessment and safeguarding."); Zhang et al., *supra* note 10, at 1-3.

[97] *See* discussion *infra* Section II.

[98] DeLiema, *Exposed to Scams* et al., *supra* note 39, at 14 (individuals whom scammers contact via social media or a website have "high engagement and victimization rates"). For a discussion of technology and elder financial exploitation generally, *see* Zhang et al., *supra* note 10.

[99] *See* U.S. INST. PEACE, TRANSNATIONAL CRIME IN SOUTHEAST ASIA: A GROWING THREAT TO GLOBAL PEACE AND SECURITY 13-14, 18 (2024); *see also* Siu, *supra* note 91 (describing the role of international criminal syndicates in internet crime against people living in Hong Kong).

[100] *See* U.S. INST. PEACE, *supra* note 99, at 27, 35 (noting Myanmar, Laos, and Cambodia in particular house call centers where thousands of workers engage in large-scale scam operations); UNITED NATIONS OFF. ON DRUGS AND CRIME, CASINOS, CYBER FRAUD, AND TRAFFICKING IN PERSONS FOR FORCED CRIMINALITY IN SOUTHEAST ASIA 15-19 (2023) [hereinafter UNODC REPORT], https://www.unodc.org/roseap/uploads /documents/Publications/2023/TiP_for_FC_Policy_Report.pdf [https://perma.cc/U8WY-R4ST]. Fraudulent offshore call centers are located in other foreign countries as well. For example, in collaboration with authorities in India, the FBI prosecuted a tech support scam based in India that laundered money through a family located in Iowa. *See* FED. BUREAU OF INVESTIGATION, 2023 INTERNET CRIME REPORT, INTERNET CRIME COMPLAINT CTR. 15, 16, (2023), https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf {https://perma.cc/ 2MAW-SHLW].

[101] *See* UNODC REPORT, *supra* note 100, at 7.

[102] *See id.* at 11-13 (describing how trafficking victims are recruited to work at scam mills).

families, and forced to perpetrate fraud.[103] Workers who have escaped tell harrowing stories of imprisonment, forced labor, and torture.[104]

Not all scams against older adults in the U.S. originate abroad, with numerous home-grown fraud enterprises also victimizing enormous numbers of people during COVID.[105] Yet it is worth noting the extraordinary scale of the international schemes. One estimate suggests that as many as half a million people worked in the industry's offshore centers in 2023, looting $63.9 billion from victims around the world.[106]

Only a few years have passed since the COVID pandemic began, and further research is imperative to fully unpack the range of factors contributing to the rise in fraud and scams. As these inquiries move forward, Routine Activity Theory provides a helpful framework for considering how the pandemic created a perfect storm. Increased online activity brought isolated older adults into contact with motivated, organized criminal actors, most of whom were physically located far away from their unsuspecting targets. Without suitable guardians to intervene, the criminal actors caused billions of dollars in harm to their victims.

II. AGING SERVICES NETWORK

As fraud increased during the pandemic, local aging services agencies stepped in to help their older clients to avoid scams, and to begin the recovery process. The U.S. Aging Services Network ("the Network") was created in 1973 to facilitate local implementation of the Older Americans Act of 1965 (OAA).[107] The U.S. Administration on Aging, which is a sub-agency within the U.S. Department of Health and Human Services, sits at the head of the Network.[108] The Network also includes State Units on Aging and Area Agencies on Aging (AAAs).[109] Most AAAs in Massachusetts also serve as Aging Service Access

[103] *See* UNODC REPORT, *supra* note 100, at 13-15; Isabelle Qian & Pablo Robles, *Duped, Trapped Then Tortured in Scam Camp*, N.Y. TIMES (Dec. 20, 2023), at A1.

[104] *See* UNODC REPORT, *supra* note 100, at 13-15 (describing how supervisors coerce trafficking victims to meet quotas by using isolation, fines, physical abuse, sexual exploitation, and threats to sell organs, or to sell the victims to other scam mills or to brothels); *see also* Cezary Podkul, *Human Trafficking's Newest Abuse: Forcing Victims Into Cyberscamming*, PROPUBLICA (Sept. 13, 2022), https://www.propublica.org/article/human-traffickers-force-victims-into-cyberscamming [https://perma.cc/J3SJ-YSTM].

[105] *See* FED. TRADE COMM'N, *supra* note 49, at 14 (describing case resolution involving tech support scheme)*; see also* Jaclyn Diaz, *Jen Shah, 'Real Housewives' Star, Sentenced to 6 1/2 Years for Telemarketing Fraud*, NAT. PUB. RADIO (Jan. 8, 2023), https://www.npr.org/2023/01/06/1147452652/jen-shah-real-housewives-star-sentenced-fraud [https://perma.cc/S9NB-KUVP].

[106] U.S. INST. PEACE, *supra* note 99, at 26 tbl. 1.

[107] Gallo & Wilber, *supra* note 14, at 153.

[108] *Id.* at 152-53.

[109] *Id.* at 152. The State Agency on Aging for Massachusetts is the Executive Office of Elder Affairs. *See Protecting Older Adults from Abuse*, COMMONWEALTH MASS.,

Points (ASAPs), which are created by state law "to assist [Medicaid-eligible] elders in maintaining their residences in the community."[110]

AAAs form the backbone of the Network and include both public agencies and private, non-profit organizations.[111] There are over 600 AAAs throughout the country.[112] Pursuant to the OAA, they provide services in five primary areas: caregiving; nutrition, including meal delivery; health and wellness; elder rights, including abuse prevention; and a variety of other "supportive services" on the basis of local community needs.[113] Services may be provided either directly, or through contracts with other public and private providers.[114]

---

https://www.mass.gov/protecting-older-adults-from-abuse (last visited Dec. 8, 2024); *see also Alzheimer's Association Map Through the Maze Exhibitor Hall – Massachusetts Executive Office of Elder Services*, ALZHEIMER'S ASS'N, https://www.alz.org/manh/events/map-through-the-maze/sponsor-exhibitor/exhibitors/ma-executive-office-of-elder-affairs (last visited Sept. 27, 2024).

[110] *See* Mass Gen. Laws ch. 19A, § 4B (2003). Some entities are both AAAs and ASAPs; and some are either one type of agency, or the other. *Compare Aging Services Access Points (ASAPs) in Massachusetts*, COMMONWEALTH MASS., https://www.mass.gov/location-details/aging-services-access-points-asaps-in-massachusetts (last visited Sept. 27, 2024) (list of Massachusetts ASAPs), *with Aging Services Access Points Area Agencies on Aging by Region*, MASS HOME CARE (Jan. 2, 2020), https://masshomecare.info/wp/wp-content/uploads/2020/09/ASAP-AAAs-by-City-Town-September-2020.doc [https://perma.cc/75DN-3LTC] (list of Massachusetts AAAs and ASAPs).

[111] *See Aging Services Network*, COMMONWEALTH MASS., https://www.mass.gov/councils-on-aging-senior-centers [https://perma.cc/LZH8-B2C2] (last visited Sept. 28, 2024); 42 USCA § 3025(a)(2)(A) (2016) (noting State agency in charge of providing for the elderly shall designate "a public or private nonprofit agency or organization as the area agency on aging").

[112] *See* #AAAS AT WORK, *supra* note 14, at 6. For a list of AAAs and ASAPs in Massachusetts, *see* MASS HOME CARE, *supra* note 109. In Massachusetts, organizations that are designated as AAA also may house Adult Protective Services (APS). *See, e.g.*, *Protective Services*, AGESPAN, https://agespan.org/solutions/safety./#:~:text=Under%20Massachusetts%20law%2C%20AgeSpan%20is,and%20to%20prevent%20a%20recurrence [https://perma.cc/WG95-7NYM] (last visited Dec. 8, 2024); *Protecting Elders At Risk of Abuse*, SPRINGWELL, https://springwell.com/service/protecting-elders-at-risk-of-abuse/ [https://perma.cc/2DAH-2VJK] (last visited Dec. 8, 2024); *see also* Adult Protective Services Functions and Grant Programs, 88 Fed. Reg. 62503, 62510-11 (U.S. Dep't of Health and Hum. Servs. proposed Sept. 12, 2023) (to be codified at 45 C.F.R. pt. 1324). APS programs are charged with investigating and addressing incidents of mistreatment against older adults and adults living with disabilities. *See National Voluntary Consensus Guidelines for State Adult Protective Services Systems*, U.S. ADMIN. FOR CMMTY. LIVING (2020), https://acl.gov/sites/default/files/programs/2020-05/ACL-Guidelines-2020.pdf [https://perma.cc/AE77-XL3C]. APS programs often address financial exploitation of older adults, typically focusing on the most egregious incidents. *See* DeLiema, *Elder Fraud and Financial Abuse*, *supra* note 23, at 708. APS generally would not become involved on a frequent basis with the more common types of frauds and scams that are the focus of this Article.

[113] Gallo and Wilber, *supra* note 14, at 154.

[114] *See Aging Services Network*, *supra* note 110. AAAs may depend on support from

Many AAAs partner with municipal agencies that serve a smaller geographic area. In Massachusetts, this includes the Commonwealth's 350 Councils on Aging (COAs), which have been described as the "front door" of services and supports for older residents and those who care for them."[115] COAs are town- and city-based agencies that receive municipal, state and federal funding to provide services such as transportation, meals, counseling, and fitness and other recreational activities.[116] COAs also offer assistance with public benefits, health insurance, and personal financial counseling.[117] Almost all Massachusetts COAs are connected with a senior center that provides both a social gathering place and a central location for obtaining information about services available in the community.[118]

When the COVID pandemic began in March 2020, aging services providers faced increased and evolving client needs, while lockdowns restricted their traditional channels of service delivery.[119] Despite these challenges, most AAAs and COAs were able to continue serving their clients.[120] Some agencies continued providing services in person, often with adjustments to address staff and client COVID-related safety concerns.[121] Many agencies expanded remote services and programming.[122] They also prioritized programs to address increasing social isolation, such as daily check-in calls and group online programming.[123] These types of activities can be critical to helping individuals maintain levels of engagement and activity that foster healthy aging.[124]

volunteers, many of whom are themselves older adults. #AAAS AT WORK, *supra* note 14, at 17, 20.

[115] Ceara Somerville et al., *Responding to COVID-19: How Massachusetts Senior Centers are Adapting*, CTR. FOR SOC. AND DEMOGRAPHIC RSCH. ON AGING PUBL'NS 1 (2020), https://scholarworks.umb.edu/cgi/viewcontent.cgi?article=1044&context=demographyof aging [https://perma.cc/78SQ-XJ2Q]. *See also* WILLIAM J. BRISK & ET AL., MASSACHUSETTS ELDER LAW § 108 (2d. ed. 2019).

[116] *See Aging Services Network*, *supra* note 111.

[117] *See* Somerville et al., *supra* note 115, at 1; BRISK, *supra* note 115.

[118] *See Aging Services Network*, *supra* note 111; Somerville, *supra* note 115, at 1.

[119] In a national survey of AAAs taken in May 2020, 93% reported serving more clients, and 69% reported increased need among existing clients since the beginning of the pandemic. *See* #AAAS AT WORK, *supra* note 14, at 5.

[120] *See id.* In a survey of Massachusetts COAs that was conducted from April through May of 2020, 91% reported that they were "continuing to provide limited programming or essential services to the community," but 6% reported that they were closed. *See* Somerville et al., *supra* note 115, at 2.

[121] For example, many AAAs that provided congregate meals prior to the pandemic were able to expand home-delivery and "grab-and-go" services to include clients who previously received their meals in-person. *See* #AAAS AT WORK, *supra* note 14, at 10.

[122] *See id.* at 12.

[123] *Id.* at 8 (60% of AAAs stated that they were "already seeing the negative health effects of social isolation on the older adults they serve.").

[124] *See generally* Sheila Novek et al, *Social Participation and its Benefits*, CENTRE ON

Technology-based service delivery offered many advantages, but it also posed challenges for some organizations and the individuals relying on them.[125] Not all aging services providers had sufficient resources or support to make the transition smoothly.[126] Because many older adults lack access to the internet, they also continued to rely on non-digital media, such as the telephone and cable access television.[127]

III. AGING SERVICES SURVEY

The authors distributed an electronic survey to aging services organizations across Massachusetts via email in May 2022 to learn how fraud and scams were impacting their operations and their clients.* The project was funded by an Academic Research Grant from the Albert & Elaine Borchard Foundation Center on Law and Aging. This section describes the survey's development, distribution, and key findings.

A. *Survey Development and Distribution*

The survey was developed with the goals of understanding the experiences of Massachusetts aging services providers with fraud and scams and learning about emerging best practices for prevention and response. The research team developed and distributed the survey with feedback from community partners including Massachusetts Councils on Aging (MCOA), the Massachusetts Executive Office of Elder Affairs (EOEA), and Greater Boston Legal Services (GBLS).[128]

A copy of the survey questions is included in the Appendix to this Article. Respondents were asked about the experiences of their organizations and their clients with fraud and scams during the pandemic, including: the frequency of reports of fraud and scams by clients, and whether this reflected change since the period prior to the pandemic; what measures the organization was taking in response to fraud and scams; experiences with reporting processes; what outside resources were available to the organization to assist clients; and what additional resources would have been helpful.[129] The survey included both multiple-choice and open-ended questions.[130]

AGING (2013), https://umanitoba.ca/centre-on-aging/sites/centre-on-aging/files/2021-02/centre-aging-research-publications-report-social-participation-and-its-benefits.pdf [https://perma.cc/C74M-FZUL].

[125] *See* #AAAS AT WORK, *supra* note 14, at 23.

[126] *Id.*

[127] *Id.*; *see also* Somerville et al., *supra* note 115, at 4.

*Survey results are on file with the authors.

[128] The survey also was submitted to the University of Massachusetts Boston Institutional Review Board, which determined that it was exempt from review.

[129] *See infra* Appendix.

[130] *Id.*

Distribution and analysis were conducted using Qualtrics survey software. A total of 416 individuals were contacted via email and asked to participate. These individuals worked for AAAs, ASAPs, COAs, and legal services organizations that specifically serve older people. These participants were selected because of the likelihood that their staff would have encountered clients who either were targeted or fell victim to fraud and scams during the pandemic.

The survey was open from May through July 2022. By the time that the survey was distributed, stay-at-home orders had been lifted, vaccines were available, and most aging services organizations had returned to providing in-person services.[131] Over 90% of the survey respondents indicated that their organizations were providing services in-person at the time of the survey administration.[132]

Responses were received from 209 participants, constituting a response rate of 50%.[133] These respondents work for organizations that are located in 186 cities and towns of Massachusetts, including organizations in each of the Commonwealth's fourteen counties.[134] Just under three quarters of respondents indicated that they worked for either a COA, senior center, or community center.[135] An additional 16% reported working for an AAA or an ASAP.[136] Other respondents worked for legal services organizations, police departments, or other types of organizations providing aging services.[137] The large majority of the responses were completed by individuals who described themselves as serving in leadership or executive roles.[138]

After the survey closed, Qualtrics was used to tally the responses. Two members of the research team reviewed the narrative responses to manually identify and classify common themes. Disagreements about classifying narrative responses were reviewed and resolved to reach a consensus.

[131] *See* McCarthy *supra* note 94; Section II.

[132] *See* Summary Results at Question 5.

[133] See *id.* at Question 3.

[134] *Id.* at Question 1.

[135] *See id.* at Question 2.

[136] *Id.*

[137] *Id.* Survey recipients were able to share the survey link with others and, as a result, some respondents worked for organizations other than AAAs, ASAPs, COAs, and legal services organizations.

[138] *See* Summary Results at Question 3. Because Councils on Aging tend to be thinly staffed, even staff in leadership or executive roles likely would have some direct contact with individual clients of the organizations. *See* Somerville et al., *supra* note 115 at 6-7.

B. *Survey Findings*

1. Almost all respondents knew of clients who had been involved with a scam

Almost 90% of respondents indicated that they had encountered one or more older clients who had been victimized by a financial scam during the pandemic.[139] Forty-seven percent believed that the number of scams targeting their clients had increased during the pandemic, while one third believed that the numbers had stayed about the same.[140]

Many narrative responses provided details about specific types of scams that were committed against the respondents' clients. Confidence scams (including romance scams and grandparent/grandchild scams) were mentioned most frequently, followed by government impersonator scams; phishing-type scams; and scams asking the target to claim money from a lottery, sweepstakes, or inheritance.[141] Descriptions of government imposter scams mentioned numerous agencies and programs, including the Internal Revenue Service, Medicare, and Social Security.[142] A few responses stated that scammers impersonated the online retailer Amazon.[143] One respondent described how a scammer impersonated the local power department in communications to an older resident.[144] A number of responses described tech support scams, in which a scammer fraudulently notifies someone that their computer needs maintenance.[145]

In one noteworthy incident, scammers tried to defraud older adults by hijacking the well-intentioned efforts of an aging services organization.[146] The

[139] *See* Summary Results at Question 8 (87% of respondents who shared the number of times since the pandemic began that they "learned of an older client who has been victimized by a financial scam" indicated a number greater than zero).

[140] *See id.* at Question 9.

[141] *See* Summary of Narrative Responses at Question 10.

[142] *See* Survey Responses at Question 10, response number 26 (IRS); response 43 (Medicare); and response 49 (Social Security Administration).

[143] For example, a respondent described the following scenario:

> "A woman was called by [someone impersonating Amazon, who claimed] her account had been hacked and she needed to pay them to reinstate it. She was instructed to purchase a gift card for its max[imum] amount and read them the numbers over the phone. She was stopped before purchasing the card. "*Id*., response 227.

[144] In this scam, the perpetrator told a town resident that "if she did not pay immediately her power would be shut off. She was told [she] had pay with prepaid gift card over the phone." According to the respondent, the municipal utility company sent a communication to all customers informing them of the scam. *See id*., response 94.

[145] Tech support scams were mentioned less frequently than confidence scams, government impersonator scams, phishing scams, or lottery/sweepstakes/inheritance scams. *See* Summary of Narrative Responses at Question 10.

[146] *See* Survey Responses at Question 10, Response 89; Rich Harbert, *Phone scam uses recording of Plymouth senior center director*, WICKED LOCAL OLD COLONY MEMORIAL (Mar.

incident—which also was described in a local newspaper—reportedly involved a scammer fraudulently re-using a recording of the town's senior center director that had previously been sent as a public service robo call to provide information to users of the center. Upon learning of the scam, the senior center sent out a new message to warn recipients about the fraud.[147]

2. Respondents described mixed experiences reporting incidents to law enforcement

Although about half of respondents indicated that they had reported a scam and were either very satisfied or somewhat satisfied, others were less positive about the experience.[148] About one third reported that they were neither satisfied nor dissatisfied, and close to 10% reported that they were either somewhat or completely dissatisfied.[149]

Several narrative responses described a sense of futility with respect to the reporting process.[150] They noted that even when they reported incidents, their clients were unlikely to recover the money they had lost.[151] A few respondents noted that they had not heard back from the law enforcement agencies to whom they made their reports.[152] Other responses described positive reporting experiences with certain agencies, and also noted situations where clients were able to recover money.[153]

One respondent explained that their organization was not certain where to report incidents. This respondent elaborated: "scams are everyone's job and no

31, 2021), https://www.wickedlocal.com/story/old-colony-memorial/2021/03/31/phone-scam-uses-plymouth-senior-center-directors-recorded-voice/4826455001/ [https://perma.cc/6TSX-LD6E].

[147] *See* Harbert, *supra* note 146.

[148] Survey Responses at Question 12a.

[149] Summary Results at Question 12a.

[150] For example, one respondent stated, "[y]ou know there is nothing that can really be done, yet you report it anyway." *Id.* at Question 12a, response 257.

[151] One respondent stated, "There is never a good resolution if someone has already sent money. It's impossible to get back and seemingly no way to prevent it from happening again. It's frustrating!" *Id.* at Question 12a, response 245. Another said that "[t]he likelihood of the senior's large amount of money being recovered was unlikely." *Id.* at Question 12a, response 202. Said another, "Once the money has moved, it is impossible to get back. I'm not satisfied with that but understand the constraints." *Id.* at Question 12a, response 45.

[152] One respondent noted that "[s]ometimes the cases are passed around or response time is too long." *Id.* at Question 12a, response 256. Another noted that the state Attorney General's Office "was excellent for one case," but also shared their opinion that "not much can be done by local police." *Id*. at Question 12a, response 32.

[153] *See id.* (commenting positively on experience reporting to state Attorney General). One respondent said they were "sorry [their client] lost the initial sums but thankful she recovered the last." *Id.* at Question 12a, Response 157.

one's job. There are multiple places to report, but I'm never sure where the right place is . . . and what the follow up is that they are supposed to do."[154]

3. Client education was the most common preventive approach

Respondents were asked to describe what services their organizations provided to help prevent clients from becoming scam victims. The most common was education for clients, with over two thirds of the responses describing speakers, workshops, written materials, or some other type of client education.[155] Numerous responses described using regular newsletters to share information about avoiding scams.[156] Many described speakers, workshops, or other live training offered in conjunction with partner organizations.[157] About 40% of the responses described partnerships with law enforcement.[158] A handful of respondents indicated that their organizations had established partnerships with banks to address the risks to their clients.[159]

Respondents were asked what, in their opinions, were good approaches to prevent financial fraud and scams. In their narrative answers, education, training, and increasing client awareness were the approaches most frequently cited.[160] Numerous respondents indicated that training must be consistent and repeated to be effective.[161] Several noted the importance of making any training relatable to participants, and of reducing the negative stigma associated with scams.[162]

---

[154] *Id.* at Question 15, Response 61.

[155] *See* Summary of Narrative Responses at Question 14.

[156] *See, e.g.*, Survey Responses at Question 8, Response 110 and Question 14, Response 117; *see also* Summary of Narrative Responses at Question 14.

[157] *See* Summary of Narrative Responses at Question 14. For example, a respondent described a "[m]onthly '"Cops & Coffee"' hour where elders can come in and learn about /discuss scams." Survey Responses at Question 14, Response 19. Another respondent described a partnership with their county's District Attorney to provide client training. *Id.* at Question 14, Response 18.

[158] *See* Summary of Narrative Responses at Question 14; *see also* responses cited *infra* note 159.

[159] *See* Summary of Narrative Responses at Question 14; *see also* Survey Responses at Question 14, Response 46, and Response 57 (mentioning seminars, bi-annual programs presented in conjunction with banks).

[160] *See* Summary of Narrative Responses at Question 18.

[161] *See e.g.*, *id.* at Question 18, Response 156 (recommending "consistent reminders to people to not trust methods of communication and verify the source of requests,") and Response 195 ("Constant education is vital!!!").

[162] *See* Survey Responses at Question 15, Response 91 ("[I] find it hard as sometimes the older adults will say '"we know about scams"' or '[I wouldn't] fall for that"'! [M]akes me think they sometimes shut their mind to it. [W]e need to overcome the stigma [] and embarrassment."); Question 18, Response 109 (noting it is easier to get older adults to "relate" to training when "personal experiences [are] shared").

For example, one response explained that their organization's "best trainings" involved role-playing by participants, because passive informational materials cannot "replicate what the actual scam is like."[163] At the interactive training, "many [participants] admitted to being scammed when they never had before."[164]

4. Aging services staff expressed frustration

Several respondents expressed concern that their efforts to educate clients were not changing behavior.[165] A number of comments observed that even individuals who are well-versed in the risks may nonetheless engage with scammers—or, as one respondent stated, "even the most educated can be taken."[166] Stated one respondent, "I think [our clients] understand the concept of all the scams but unfortunately due to loneliness, boredom, forgetfulness, or not wanting to be rude, they talk to [scammers] who seem kind on the phone."[167] Another stated: "sometimes the older adults will say 'we know about scams' or 'I wouldn't fall for that!' [It] makes me think they sometimes shut their mind[s] to it. We need to overcome the stigma [] and embarrassment."[168] This respondent suggested that people who have been harmed by scams could help others by sharing their experiences.[169]

Other comments expressed the need to reach older people who are either less involved or not involved at all with their local aging services organizations. [170] One respondent specifically identified older people who are homebound and people with limited English proficiency as less likely to receive their organization's materials on scam prevention.[171]

In addition, numerous responses expressed skepticism about law enforcement's ability to stop fraud from occurring and recover lost funds.[172]

[163] Survey Responses at Question 18, Response 63.

[164] *Id.*

[165] *See* Summary of Narrative Responses at Question 15; *see e.g.*, Survey Responses at Question 15, Response 23, Response 91, and Response 240.

[166] Survey Responses at Question 15, Response 33.

[167] *Id.* at Question 15, Response 240.

[168] *Id*. at Question 15, Response 91.

[169] *Id*.

[170] For example, one response observed that "it's hard to know if everyone reads our newsletters, looks at our messages online, etc. People that are active in the center are educated often; I have more concern for the seniors in town that are not active in our center." Survey Responses at Question 15, Response 32. Another noted that "[o]nly those who attend our events hear [the organization's fraud and scams outreach] on a regular basis." *Id.* at Question 15, Response 24.

[171] One respondent expressed the desire to "[h]ave better outreach to those who are homebound or who do not speak or read English." *Id.* at Question 15, Response 4.

[172] *See* Summary of Narrative Responses. For example, one respondent wrote "you know there is nothing that can really be done, yet you report it anyway." Survey Responses at Question 12a, Response 257. Another stated that "Reporting to law enforcement usually does

One respondent wrote, "There is nothing our organization can do [beyond] what we are [doing]. It is really up to the government to stop these attacks . . . and prosecute to the fullest extent of the law. You don't see much of this happening."[173] This sentiment was echoed by many others who also wrote about the need to stop the perpetrators of these incidents.[174]

IV. DISCUSSION AND RECOMMENDATIONS

A. *Limitations of the Survey*

The survey results illuminate aging service providers' perspective on the pandemic's wave of fraud against older people. The 50% response rate is notably high, given the operational challenges during the summer of 2022 due to the continuing pandemic.[175] There are, however, some limitations of the study, and caution should be exercised in generalizing the results. Because the survey was distributed electronically, it may include a greater proportion of responses from aging services personnel who are more comfortable with technology, or who were simply better able to keep up with electronic messages during the period when the survey was open.

The survey was conducted in Massachusetts because the principal investigators are affiliated with the University of Massachusetts Boston's Gerontology Institute and were able to leverage the Institute's existing relationships with the Massachusetts aging services network. However, states experienced the impacts of COVID-19 differently across the course of the pandemic, which could limit the broader applicability of the findings beyond Massachusetts.[176]

not result in any closure." *Id.* at Question 15, Response 47. In response to Question 15, "What do you wish your organization could do to prevent frauds and scams," one respondent stated, "Good question. Stop it from happening in the first place. Money is gone, never returned once you've paid a scammer. Identity theft can happen to anyone, even those who have some awareness of the possibility." *Id.* at Question 15, Response 27.

[173] Survey Responses at Question 15, Response 137.

[174] *See, e.g.*, Survey Responses at Question 15, Response 17 ("Unless or until there are federal or state resources to stop scammers, the most important issue is how to prevent someone from being taken advantage of."); Question 15, Response 131 ("Catch the criminals and heavily publicize it in the media and how they did it."); Question 15, Response 22 ("[K]nowing that those doing it would be prosecuted would go a long way to making people feel better."); Question 17, Response 5 ("[M]ore ability for law enforcement to catch and prosecute offenders" would help).

[175] For a discussion of the challenges faced by aging services providers during this period, *see supra* notes 119-127 and accompanying text.

[176] *See* William H. Frey, *One Year In, COVID-19's Uneven Spread Across the U.S. Continues*, BROOKINGS (Mar. 5, 2021), https://www.brookings.edu/articles/one-year-in-covid-19s-uneven-spread-across-the-us-continues/ [https://perma.cc/NJG8-GTU9].

B. *Comparisons with National Data*

The high number of respondents whose clients had encountered a scam was consistent with federal government data showing a sharp increase in incidents during the period.[177] Forty-seven percent of survey respondents indicated that they believed these numbers had climbed since the time prior to the pandemic, suggesting that the national upward trends were visible to many, but not all, of these local entities.[178]

Whereas the national data reported in Section I is based on individual reports to federal agencies,[179] the information collected through the survey consists of second-hand reports shared by social service providers about their clients.[180] This is a fundamentally different method of measuring and understanding fraud based upon the direct point-of-view of the providers, rather than the individuals targeted. The survey responses undoubtedly exclude important details about these incidents that were not shared with the providers, and therefore were not reported through the survey. Also missing from the survey are those incidents that clients chose not to share with their local aging services organization.[181]

Despite these limitations, future, periodic surveys of aging services organizations could help supplement the imperfect data generated from direct reports to government agencies.[182] Some victims may share experiences with trusted staff at their local aging services organization that they do not report to local police, to the FBI, or to the FTC. If so, then the information collected by aging services may capture incidents that are excluded from other data sets.[183]

C. *Education Through Aging Services Providers*

Respondents indicated that client education is a best practice and also a significant focus of their efforts to prevent fraud.[184] Even prior to the pandemic, many providers featured educational programming on financial exploitation and

[177] *See supra* notes 32–38 and accompanying text.

[178] *See supra* note 140 and accompanying text.

[179] *See supra* notes 42–48 and accompanying text (explaining that data based on individual reports likely underrepresents the true number of scams).

[180] *See* discussion *supra* Section III.A (describing survey participants).

[181] As noted previously, respondents may not wish to report incidents due to shame and embarrassment. *See supra* notes 42-45.

[182] Elder abuse research has used assessments conducted by health care and other service providers. For a discussion of the potential opportunities and challenges of using second-hand reports on elder abuse, *see* Scott R. Beach et al., *Screening and detection of elder abuse: Research opportunities and lessons learned from emergency geriatric care, intimate partner violence, and child abuse*, 28 J. ELDER ABUSE NEGL. 185, 187-88 (2016).

[183] *See id.* Secondhand reports are filtered through the lens of the service provider, and the provider's subjective view of a situation may differ from the experience of the individual victim. *See id.* at Table 1 (citing differing viewpoints as a challenge to using health care provider screening to accurately identify elder abuse).

[184] *See supra* notes 155-64 and accompanying text.

related topics among their offerings to clients and were prepared to continue serving in this role.[185] Their belief in education as a best practice aligns with studies finding that teaching consumers about scams can reduce the likelihood that they will engage with scammers or lose money.[186] One study funded by the FINRA Investor Education Foundation[187] found that consumers who were armed with knowledge of specific types of scams were 80% less likely to engage with them; and that, if they did engage, they were 20% less likely to lose money.[188]

This and other research provide insight into how thoughtful design can maximize the impact of training.[189] For example, training should be both (1) "scam-specific," and (2) "directed to individuals who have a set of characteristics that make them particularly vulnerable to that type of scam."[190] The most effective interventions address mental frames that enhance vulnerability, in addition to providing descriptive information about specific scams.[191] For example, people who are inclined to trust authority are more likely to fall victim to government imposter scams, so training about such scams should teach participants that it is important to verify the identity of anyone who claims to work for the government.[192] People who are confident in their

[185] *See* USAGING, 2020 AAA NATIONAL SURVEY REPORT: MEETING THE NEEDS OF TODAY'S OLDER ADULTS 8 (2020), https://www.usaging.org//Files/AAA-Survey-Report-new-identity-508.pdf [https://perma.cc/R79D-F9KY] (85% of surveyed AAAs provided community training about elder abuse, and 62% provided training specifically on financial abuse).

[186] *See* HONICK ET AL., *supra* note 41, at 26; *see also* DeLiema et al., *Exposed to Scams*, *supra* note 39, at 11-12 (survey found that 30% of respondents who did not engage knew about the scam before they were targeted compared to 12% of people who engaged but were not victimized).

[187] The Financial Industry Regulatory Council (FINRA) operates under the supervision of the U.S. Securities and Exchange Commission to regulate FINRA member companies, including broker dealers. The FINRA Investor Education Foundation funds initiatives related to "financial capability and fraud prevention." *See* FIN. INDUS. REGUL. COUNCIL, 2022 FINRA ANNUAL FINANCIAL REPORT 3, 6 (2023) https://www.finra.org/sites/default/files/2023-06/2022_Annual_Financial_Report.pdf [https://perma.cc/3ZA5-ZRLW].

[188] *See* HONICK ET AL., *supra* note 41, at 26.

[189] The FINRA Investor Education Foundation has supported research into the risk factors for fraud and the pedagogical approaches that are most effective at reducing individual risk. *See* HONICK ET AL., *supra* note 42, at 26; MARGUERITE DELIEMA ET AL., DOES ONE SIZE FIT ALL? AN EXAMINATION OF RISK FACTORS BY SCAM TYPE 5 (FINRA Inv. Education Found., Capability 2022); DeLiema et al., *Exposed to Scams*, *supra* note 39; *see also* DeLiema et al., *supra* note 87, at 1055-56.

[189] *See* HONICK ET AL., *supra* note 41, at 27.

[190] DeLiema et al., *Exposed to Scams*, *supra* note 39, at 5; *see also* DeLiema et al., *Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type*, *supra* note 87, at 1055-56.

[191] *See* HONICK ET AL., *supra* note 41, at 26-27.

[192] *See id.* at 26.

investing abilities are more likely to fall for investment scams, so training about investment scams should teach participants to investigate thoroughly when considering any new financial opportunity, even if they believe they already understand it.[193]

Developing sophisticated training materials incorporating the latest research requires specialized expertise that few aging services providers will have in-house. As described in Section II, many agencies are thinly staffed, under-resourced, and rely on outside contractors and volunteers to provide services.[194] While existing newsletters and programming can be effective channels to distribute information, providers require additional resources and outside help to maximize the quality and effectiveness of their messaging.

On the other hand, local providers are well-situated to tailor content and means of delivery based on their knowledge of their local communities.[195] For example, they can assess the needs of their clientele for materials that are linguistically and culturally appropriate, and that are provided in accessible formats.[196] The recommendation to provide training to clients with limited English proficiency also points to the need to make information available equitably across the diverse populations accessing aging services.[197]

D. *Perceptions of Enforcement Trends*

Several respondents suggested that law enforcement should do more to prevent crimes before they occur, to catch and prosecute the perpetrators, and to return funds to the victims.[198] Although the large majority of these crimes go unsolved, federal enforcement agencies have, in fact, reported a number of civil enforcement successes since the COVID pandemic began, including several that have returned money to victims.[199] The Department of Justice also continues to

---

[193] *See id.* at 21-23.

[194] *See supra* Section II.

[195] *See* USAGING, *supra* note 185, at 6 ("[AAAs] respond to the unique needs, challenges and demographics of the older adults in the communities they serve.").

[196] *See id.* at 6–7 (53% of AAAs provide "translator/interpreter assistance").

[197] *Id.*

[198] *See* survey responses discussed *supra* note 174.

[199] *See, e.g.*, FED. TRADE COMM'N, PROTECTING OLDER CONSUMERS 2021-2022: A REPORT OF THE FEDERAL TRADE COMMISSION 11 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P144400OlderConsumersReportFY22.pdf [https://perma.cc/L68M-JZYT] (describing almost $300,000 in remediation paid to mostly older consumers who, the FTC alleged, paid "large sums" to Elite IT Partners, Inc. after "intimidation and scare tactics" convinced them to purchase unnecessary tech support services); *id.* at 12 (describing $1.8 million in remediation to consumers who allegedly paid the company Lifewatch Inc. for medical alert systems that had been advertised as free in telemarketing calls); *id.* at 14 (describing $23 million settlement in a case against MOBE Ltd., alleging that MOBE's advertisements stated that their program was "A Surefire Way To Create A Six-Figure Retirement Income In Less Than 12 Months."). DOJ and FTC also returned $115 million to consumers, including many older people, through a forfeiture by the company MoneyGram in connection with a deferred

prosecute numerous scams targeting older people, with noted cases involving romance, grandparent, and tech support scams, among others.[200] While there is much room for additional progress—particularly in the area of international enforcement—the common perception that law enforcement efforts are completely stymied is inaccurate.[201]

Furthermore, prompt reporting to both law enforcement and financial institutions is vital to reducing losses and recovering funds.[202] In some instances, fraudulent transactions may be halted before funds have left the custody of the victim's financial institution.[203] In 2018, the FBI established the IC3 Recovery Asset Team, which facilitates communication between FBI field offices and financial institutions.[204] Complaints received by the FBI are entered into a database that is analyzed to identify trends in suspicious activity.[205] In addition, some complaints are shared with financial institutions to attempt to

prosecution action that had been entered with the company several years earlier. *See* Press Release, U.S. Dep't of Just., Nearly 40,000 Victims Receive Over $115M in Compensation for Fraud Schemes Processed by MoneyGram (Feb. 10, 2023), https://www.justice.gov/opa/pr/nearly-40000-victims-receive-over-115m-compensation-fraud-schemes-processed-moneygram#:~:text=In%20November%202018%2C%20MoneyGram%20agreed,processed%20during%20the%20DPA%20term [https://perma.cc/5ZYW-ZDUA].

[200] *See, e.g.*, Press Release, U.S. Dep't of Just., Money Launderer Sentenced for $8 Million Romance Scam Fraud Scheme (Mar. 21, 2023), https://www.justice.gov/usao-ma/pr/money-launderer-sentenced-8-million-romance-scam-fraud-scheme [https://perma.cc/DE9D-5G4Q]; Press Release, U.S. Dep't of Just., Two Defendants Sentenced for Participating in Nationwide Grandparent Scam (Nov. 17, 2022), https://www.justice.gov/usao-sdca/pr/two-defendants-sentenced-participating-nationwide-grandparent-scam#:~:text=From%20approximately%20November%201%2C%202019,for%20car%20accident%20victims%2C%20or [https://perma.cc/6V6X-ZB7V]; Press Release, U.S. Dep't of Just., Passaic County Man Charged in $13 Million Technology Support Scam Targeting over Seven Thousand U.S. Victims (Aug. 31, 2023), https://www.justice.gov/usao-nj/pr/passaic-county-man-charged-13-million-technology-support-scam-targeting-over-seven [https://perma.cc/NF86-VEL8].

[201] *See* CFPB FRAMEWORK 2022, *supra* note 9, at 19 ("Among those who do recover funds from [elder financial exploitation], reporting to an authority is often an important step. Doing so can initiate an investigation about who was responsible, which can ultimately lead to the return of their money.").

[202] *Id.*

[203] A true reversal is only possible if the perpetrator has not yet moved the funds out of the receiving account. For a discussion of how a reversal works, *see* Bruce Phillips, *The Moneys Gone – After a Successful Wire Fraud*, WFGAGENT: TECH TALK (Sept. 17, 2018), https://wfgagent.com/tech-talk/the-moneys-gone-after-a-successful-wire-fraud/ [https://perma.cc/K7N7-CTM4].

[204] U.S. DEP'T. OF JUST., ANNUAL REPORT TO CONGRESS ON DEPARTMENT OF JUSTICE ACTIVITIES TO COMBAT ELDER FRAUD AND ABUSE 60 (2022), https://www.justice.gov/media/1253691/dl?inline [https://perma.cc/T6NL-79CL].

[205] FED. BUREAU OF INVESTIGATION, 2022 INTERNET CRIME REPORT, *supra* note 32, at 9.

freeze the affected funds.[206] The FBI reports that in the twelve-month period ending June 2022, the program succeeded in freezing funds in time to prevent losses worth over $375 million.[207] Experts note that "[t]ime is of the essence," as law enforcement must act during the brief lag between the transaction's initiation and completion to quickly recover the funds.[208] The FBI urges victims to immediately contact any financial institutions involved in the transaction, and to "request a recall or reversal."[209]

Aging services providers are well-situated to urge their clients to report fraud to law enforcement and to any financial institutions involved, maximizing the likelihood of recovery.[210] Staff who mistakenly believe that reporting is useless may be less inclined to facilitate the process for their clients. Communication about rapid response efforts and enforcement successes will encourage these efforts and help change the perception among some that "there's nothing [law enforcement] can do to catch the criminals."[211]

E. *Recommendations*

This Section offers recommendations about how to elevate, support and leverage efforts by aging services in the continuing fight against fraud. While the acute challenges of COVID have abated since the survey was distributed, fraud and scams continue to grow ever more prevalent.[212] Local organizations have a wealth of knowledge about their communities, making them uniquely situated to sound the alarm to their clients and others.[213] Staff are in contact with older people every day, providing essential services and serving as trusted resources.[214] When their capabilities were strained by the pandemic, they used available internal and external resources to respond with proactive anti-fraud training and support. Yet, their descriptions of their experiences during the pandemic reflect a level of fatigue as the problem dragged on despite their best efforts.

The theme of collaboration was repeated throughout the survey responses and carries into these recommendations. Aging services were already overextended when COVID and its accompanying wave of fraud and scams arrived.[215] They

[206] *Id.*

[207] *Id.* at 10.

[208] *See* CFPB FRAMEWORK 2022, *supra* note 8, at 38. Reporting may also help law enforcement contact the victim in the event that funds become available for remediation or restitution. *Id.* at 45 ("[L]aw enforcement often interact[s] with EFE victims in ways that are critical to their prospects for financial recovery.").

[209] FED. BUREAU OF INVESTIGATION, 2022 INTERNET CRIME REPORT, *supra* note 32, at 9.

[210] *See supra* Section II.

[211] Survey Responses at Question 11, Response 29.

[212] *See* 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 5.

[213] *See supra* Section II.

[214] See supra Section II.

[215] *See* #AAAS AT WORK, *supra* note 14, at 22.

should not, and cannot, fight this battle on their own. Numerous stakeholders and systems act individually, interactively, and collaboratively to prevent financial exploitation; no one stakeholder will solve, or fail to solve, the problem on its own.[216] Rather, interactions between and among the stakeholders and systems will determine whether older people are protected from future harm.[217] Social isolation, work-from-home orders, and the shift to remote and hybrid operations posed obstacles to effective collaboration during the pandemic. As these challenges fade, stakeholders are presented with new opportunities to renew and develop partnerships.

1. Law Enforcement and Financial Services Should Enhance Their Collaborative Efforts

National law enforcement would benefit from specific, dedicated channels of communication with the Aging Services Network to facilitate cooperation in fighting fraud. The FBI should appoint an Aging Services Liaison to coordinate efforts at the national level. Quarterly or more frequent information and listening sessions will ensure that information about enforcement tools and successes reaches social services providers in the community, while also giving aging services staff the opportunity to share the latest threats and other trends that they learn through their work with older people.

All levels of law enforcement must remain committed to enhancing support for fraud victims and should ensure that they are communicating their commitment to aging services and other local community partners. Local police departments and national enforcement agencies should follow up consistently with the victims to share updates on any investigations—or, if they decide to close a matter without investigating, to explain why that decision was made. Many aging services organizations and local law enforcement already enjoy robust partnerships, collaborating on abuse prevention, client education, and other joint projects. Where these relationships are weaker, however, closer partnerships may reduce the sense of futility expressed by survey respondents.

Better coordination also would provide law enforcement with the opportunity to share their successes. Recent indictments, prosecutions, and restitution awards are a testament to the possibility of stopping the perpetrators and restoring funds to victims.[218] While they reflect only a small proportion of all incidents, they nonetheless provide encouraging evidence that fraud-fighting efforts are not in vain.[219]

Financial institutions are another critical partner for aging services providers, as both share a common interest in scam prevention.[220] Unlike the under-funded

[216] *See Elder Justice Initiative*, *supra* note 26.

[217] *Id.*

[218] *See supra* notes 192-93.

[219] *See* CFPB FRAMEWORK 2022, *supra* note 9, at 37-41, for a detailed discussion of factors that may enhance the likelihood of a monetary recovery.

[220] *See, e.g.*, J.P. MORGAN CHASE & CO., ANNUAL REPORT 2022 47 (2023),

Aging Services Network, the financial services industry spends billions of dollars each year on fraud prevention to prevent costly losses.[221] Some survey respondents described existing collaborations with banks to provide client training.[222] An expansion of these relationships would allow aging services to leverage the deep expertise of the private sector, while also providing a new channel for banks to directly educate individuals who are at risk of being targeted for fraud. Closer partnerships may also facilitate prompt reporting to financial institutions to maximize the likelihood of preventing losses.

2. Streamline the Reporting Process

Organizations that serve older people should be empowered to help their clients contact law enforcement and complete other follow-up after fraud occurs. Yet many survey respondents described confusion about how to help, and had mixed experiences with reporting.[223] The system is decentralized, and it is unclear which of the numerous national, state, and local enforcement agencies to contact.[224] Because the likelihood of recovering lost funds is low, older people and the organizations that help them may be less motivated to put in the effort to identify which agency or agencies should be notified.[225] This is an obstacle both to obtaining redress for older people and to the collection of accurate data to inform enforcement and policy making.

To address these issues, the reporting process should be streamlined and communicated to aging services organizations and others who are likely to encounter affected older people in real time, when there is some chance of recovering lost funds. This could involve single point reporting through a

https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport-2022.pdf [https://perma.cc/7XK2-PSQ5] ("While fraud is everywhere, we are improving our ability to protect customers earlier and more often. Education plays a big role, too. Bankers, Community Managers and marketing work together to help customers build healthy financial habits and avoid becoming victims of fraud.").

[221] *See* KEN FEINSTEIN ET AL., JS HELD, DETECTING FRAUD USING EMERGING TECHNOLOGY: DON'T BE AFRAID TO INNOVATE 1 (2023) ("[A] Juniper Research report on online payment fraud said merchants and financial service organizations will spend $9.3 billion annually on fraud prevention.").

[222] *See supra* note 159.

[223] *See supra* notes 151-54.

[224] One 2023 AARP consumer-facing article suggested that victims of fraud should report these incidents to three different entities: local law enforcement, the FTC, and the FBI. *See* Christina Ianzito, *Americans Think Fraud is at 'Crisis Level,' Survey Finds*, AARP (May 17, 2023), https://www.aarp.org/money/scams-fraud/info-2023/fraud-awareness-survey.html#:~:text=As%20scams%20skyrocket%2C%20AARP%20report,scam%20threat%20and%20scammers'%20methods&text=Incidents%20of%20fraud%20have%20exploded,billion%20reported %20stolen%20in%202022 [https://perma.cc/NJ5N-PRAA].

[225] *See* CFPB FRAMEWORK 2022, *supra* note 8, at 24 ("Among victims who did not report their experience to the police, one of the most common reasons for not reporting was their belief that law enforcement would not consider their experience to be worth investigating.").

national phone number, following the model of the national poison control hotline or the 988 Suicide & Crisis Lifeline.[226] The DOJ's National Elder Fraud Hotline, which was started in March 2020, could take on this role.[227] Alternatively, reporting could be coordinated among a network of state or local reporting agencies that cooperate to share resources and data. In either case, a single call by the client or caregiver would begin a process that would both inform the appropriate law enforcement agencies and connect the client with local support resources.

3. Centralize Education and Training Resources

Survey respondents indicated that the most effective training is current, frequent, interactive, and relatable, and also avoids any shaming towards people who engage with scammers.[228] Some survey respondents already partner with law enforcement, banks, or others to coordinate free or low-cost training.[229] Yet developing high-quality training materials is time consuming, as is identifying external resources. Aging services providers may have limited specialized expertise with respect to content and pedagogy. They may not be able to maintain training and educational materials that reflect the most current scams, either because they have not learned about them yet, or because they simply lack the resources to make frequent revisions to their existing materials. Staff may not have the translation skills necessary to provide training materials in languages other than English.[230]

Designating a central, national resource center to produce education and training resources about fraud would enhance efforts of local aging services programs. A resource center could employ knowledgeable instructional designers to incorporate research on adult learners, and older learners in particular, using up-to-date pedagogical approaches to maximize effectiveness. Developers could implement best practices identified by fraud researchers, such as integrating behavioral training that prepares individuals to effectively respond

[226] The U.S. Poison Control helpline is a network consisting of more than fifty poison centers located around the country. *Who We Are*, AM.'S POISON CTRS., https://www.aapcc.org / (last visited Sept. 28, 2024). The 988 Suicide & Crisis Lifeline is managed by the Substance Abuse and Mental Health Services Administration. Calls to the central number are routed to local service providers depending on the area code of the call. *See SAMHSA's National Helpline*, SUBSTANCE ABUSE AND MENTAL HEALTH SERV.'S ADMIN., https://www.samhsa.gov /find-help/national-helpline [https://perma.cc/LAK4-HGWC] (last visited Sept. 28, 2024).

[227] *See Elder Fraud & Abuse: National Elder Fraud Hotline*, U.S. DEP'T OF JUST. OFF. FOR VICTIMS OF CRIME, https://ovc.ojp.gov/program/elder-fraud-abuse/national-elder-fraud-hotline#:~:text=In%20March%202020%2C%20the%20U.S.,averaging%2083%20calls%20a%20day [https://perma.cc/HA8A-ZNAW] (last visited Dec. 8, 2024).

[228] *See supra* notes 161-64 and accompanying text.

[229] *See supra* notes 157-59 and accompanying text.

[230] *See* Gallo & Wilber, *supra* note 14, at 155 (demographic trends will call for aging services to be offered in "a variety of languages").

to scams in real life.[231] Creating multilingual materials also would help local agencies that lack their own translation resources.

The resource center could be located within an existing public agency, such as the U.S. Administration for Community Living; or placed under the aegis of a private organization with specialized expertise, such as the National Council on Aging. Alternatively, instead of a single center, a well-coordinated resource network consisting of state or regional centers could provide many of the benefits of national centralization, while also allowing for training to be tailored locally as needed.

CONCLUSION

The aging services response to COVID-19 modeled institutional flexibility in the face of uncertainty and challenge.[232] These agencies quickly pivoted to meet the new and expanded needs of their clients, including a wave of fraud and scams perpetrated with the very technologies that helped these organizations remain open despite social distancing.[233] Now, as the world continues its return to a post-COVID normalcy, it unfortunately appears that fraud targeted against older people will remain a persistent feature of the aging landscape.[234]

Moving forward, the Aging Services Network provides a unique environment to implement and test interventions for preventing and addressing fraud. Local agencies stand ready to distribute enhanced anti-fraud training and could partner with scholars and policymakers to test its effectiveness.[235] Randomized controlled trials assessing interventions would greatly enhance the currently limited knowledge of best practices, providing a roadmap for future efforts.[236]

The need for effective interventions will only grow with the rise of artificial intelligence, which adds a new level of complexity to technology-based frauds. Aging services providers and their partners will need to redouble their efforts, enhancing their own sophistication and leveraging additional resources to address the new threats. The staggering level of dollar losses over the past several years suggests that there is much work ahead.[237] Collaboration, coordination, and communication among stakeholders will be critical to meeting the challenge.

---

[231] *See* HONICK ET AL., *supra* note 41.

[232] *See generally* Gallo & Wilber, *supra* note 14.

[233] *See* #AAAS AT WORK, *supra* note 14, at 4, 11.

[234] *See* 2022 FBI ELDER FRAUD REPORT, *supra* note 2, at 5.

[235] In addition, because AAAs and COAs already provide programs to combat social isolation, they could serve as a laboratory to examine how anti-loneliness interventions may have the added positive effect of reducing susceptibility to fraud. *See* USAGING, *supra* note 183, at 9 (describing AAA efforts to "assess clients for social isolation . . . and for loneliness" and addressing both through services "encouraging socialization").

[236] AAAs already offer evidence-based programming through funding provided under the Older Americans Act for disease prevention and health promotion. *See id.* at 12.

[237] *See generally* 2022 FBI ELDER FRAUD REPORT, *supra* note 2.

APPENDIX

#	Question Text	Response Options
1	In what city or town is your organization located?	Open response
2	What is the name of your organization?	Open response
3	What is your job title?	Open response
4	Approximately how many years have you worked in aging services or legal services for older people?	Open response
5	At your COA/Senior Center or legal service, what methods are used to deliver programs and services? Check all that apply:	Check all that apply: *1. Phone; 2. Email; 3. Written materials; 4. Live video streaming (zoom, facebook live);5. Social media (Facebook, Twitter, Instagram, etc); 6. Cable access television; 7. In-person, with COVID-19 safety protocols in place; 8. Pre-recorded video; 9. Remote notary; 10. Docusign, online forms; 11. Does not apply - programs and services cancelled.*
6	Approximately what percentage of the services at your organization are provided via technology and what are provided in-person?	% Technology: open response; % In-person: open response

#	Question Text	Response Options
7	Over your entire career in aging services or legal services for older people, about how many times have you learned of an older client who had been victimized by a financial scam? (ex: lost money or personal information)	Open response
8	Since the pandemic started in March 2020 about how many times have you learned of an older client who has been victimized by a financial scam?	Open response
9	In your opinion, since the pandemic started has the number of scams targeting your clients increased, stayed about the same, or decreased, compared to the period before the pandemic?	Multiple choice: *1. Increased; 2. Stayed about the same; 3. Decreased; 4. Don't know, not sure*
10	If any of your clients have been targeted for a scam during the pandemic – please describe what happened:	Open response
11	If you have been alerted to someone who has been scammed, what did you do?	Open response
12	If you've reported financial fraud or a scam, who did you report it to?	Open response

#	Question Text	Response Options
12a	If you've reported a scam, were you satisfied with how the situation was resolved?	Multiple choice: *1. Very satisfied; 2. Somewhat satisfied; 3. Neither satisfied nor dissatisfied; 4. Somewhat dissatisfied; 5. Completely dissatisfied.*
12b	Additional comments:	Open response
13	Does your organization have staff training resources about scams?	Multiple choice*: 1. Yes; 2. No*
14	If applicable, describe any services your organization provides to help prevent your clients from becoming the victims of scams:	Open response
15	What do you wish your organization could do to prevent frauds and scams?	Open response
16	Would additional resources help your organization to protect your clients against scams? Check all that would help:	Check all that apply: *1. Training for existing staff; 2. Educational materials to give to clients; 3. Additional staffing to focus on scam prevention; 4. Internal policies and procedures about protecting clients' personal information; 5. Collaborations with legal or financial services; 6. No additional resources are needed*

#	Question Text	Response Options
17	Would additional collaboration with the groups listed below help your organization to protect your clients against scams? Check all that would help:	Check all that apply: *1. Social services providers; 2. Legal services organizations; 3. Law enforcement agencies; 4. Government agencies outside of law enforcement; 5. No additional collaboration is needed*
17a	Other:	Open response
18	What in your opinion are good approaches for financial fraud and scam prevention?	Open response
19	Please use the space below to provide any additional information that you weren't able to provide in the responses above:	Open response
20	We'd appreciate the opportunity to follow up with you via telephone. If you would be willing to speak with us, please provide your contact information:	Open response