

Mitigating the Risk of Digital Financial Exploitation

Patricia R. Recupero, JD, MD

The article by Zhang and colleagues in this issue of *The Journal* calls attention to an important but underrecognized problem facing today's seniors and their loved ones. The risk of digital financial exploitation, particularly in the wake of the COVID-19 pandemic, has risen considerably in recent years and continues to rise today. Zhang *et al.* provide a helpful analysis of assessment tools currently available to forensic psychiatrists for the evaluation of financial capacity. Although many of these tools were not originally intended to encompass technologically based transactions, the risks of fraud and scams associated with payment apps, social media, and electronic fund transfers are considerable and growing. Fraudsters frequently target vulnerable older adults, and victims have lost large sums through some of the more prevalent schemes. Several strategies can help to mitigate the risk of severe losses and to increase the likelihood that lost assets can be recovered. Proactive education through increased awareness will prove helpful, but given the growing sophistication of modern digital cons, such as romance scams, increased technological safeguards are warranted in the setting of reduced financial capacity. When losses do occur, there are some resources for recovery and for filing complaints against perpetrators.

J Am Acad Psychiatry Law 51:181–89, 2023. DOI:10.29158/JAAPL.230028-23

Key words: elder abuse; financial capacity; fraud; information and communications technology; social media

Zhang, Morris, McNeil, and Binder¹ have shed light on a topic of increasing importance and urgency as the nation's baby boomers advance into retirement and technology becomes more central to nearly every aspect of our lives. Surprisingly little research to date has explored the potentially devastating social consequences of financial exploitation in the coming years.¹ As Edersheim and colleagues² note, nearly \$60 trillion in wealth is expected to pass down from the estates of elderly individuals over the next five decades. An estimated one in 18 older adults without significant cognitive impairment falls victim to some form of financial fraud or scam each year in the United States.³ Furthermore, the number of victims of financial exploitation and fraud is expected to nearly double within the next two to three decades.² In 2021 alone, more than \$1.7 billion in losses were reported to the elder fraud

division of the Federal Bureau of Investigation (FBI), with many older adults losing more than \$100,000 in assets and an average loss of more than \$18,000 for victims older than 60 years of age.⁴ Financial exploitation represents the most common form of elder abuse,^{5–7} and older adults make up a disproportionately large share of consumer fraud victims.⁸ In their article, Zhang and colleagues¹ introduce a variety of useful tools for mental health professionals to approach the assessment of older adults' financial capacity.

Risk Factors

Zhang *et al.*¹ identified some of the risk factors for financial abuse, including decreased social support, dependence on others, and cognitive impairment, particularly with respect to the management of one's financial affairs. The relevance of specific risk variables is a nuanced matter, however. One recent study that explored relationships between risk factors and financial exploitation of older adults found that lower social support and increased social network size were associated with a higher risk for victimization.⁹ The authors of the study concluded that:

Published online May 30, 2023.

Dr. Recupero is Clinical Professor of Psychiatry, Warren Alpert Medical School, Brown University, and SVP for Education and Training, Care New England Health System, Providence, RI. Address correspondence to: Patricia R. Recupero, JD, MD. E-mail: Patricia_Recupero@Brown.edu.

Disclosures of financial or other potential conflicts of interest: None.

When it comes to the role of social relationships and risk for [financial exploitation], “more may not always be better.” Encouragement to widen the social network by “making new friends” should be stressed less than making sure these new network members will truly be supportive of the older adult (Ref. 9, p 990).

As opposed to financial exploitation in general (such as misappropriation of assets by a trusted caregiver), fraudsters and scammers appear more likely to target isolated older adults (i.e., those with no trustworthy friends or relatives to help them manage their financial assets).¹⁰ Unfortunately, the percentage of older adults who live alone is increasing.¹¹ Women and older seniors appear to be at greater risk,^{2,12} and poor numeracy (comfort with numbers) also appears to increase risk.¹³ With respect to COVID-19–related scams in particular, identified risk factors for vulnerability were primarily related to financial variables, such as concerns about finances after the pandemic and a desire for advice about money management.¹⁴

When compared with older adults who fall victim to financial abuse, elders who do not succumb to such exploitation are more likely to discuss their personal finances with a trusted individual.² Therefore, it may seem that encouraging dialogue between an older adult and a trusted loved one or fiduciary would be advisable; however, this risk variable is also nuanced. When there is a close relationship between a vulnerable adult and another person, such as an adult child of a parent with neurocognitive impairment, the risk for domestic financial abuse can be significant. Although this type of financial exploitation is less frequently reported to authorities, it likely accounts for the majority of elder financial abuse.¹⁵ Older adults themselves may be less likely to recognize financial exploitation as abuse when it is perpetrated by family members.¹⁶

Risk factors for financial exploitation are distinct from those for elder abuse in general. In one recent study, researchers found that cases involving financial abuse alone (when contrasted with cases without financial exploitation and cases involving both financial and other forms of elder abuse) had the lowest rates of identifiable risk factors.¹⁷ Therefore, trying to identify persons at greatest risk through the recognition of specific risk variables, as a single tool, may not be the most effective strategy to protect our nation’s elders from financial abuse. Awareness of early warning signs of financial exploitation, in addition to knowledge about the risk factors, may perform an important role in mitigation.

Technology

Zhang and colleagues note that scant research has explored technological risk factors.¹ As information and communications technologies continue to evolve at an unprecedented rate, technological risk factors for financial exploitation are likely to adapt at a similarly rapid pace.

Electronic payment apps and services such as Zelle, Venmo, and Cash App, whereby one can initiate an electronic funds transfer (EFT) directly from a checking or savings account, provide convenience but may also increase the risk of substantial losses. Zelle, in particular, the most popular direct-payment app, is rife with reports of fraud and scams,^{18,19} and victims are often unable to recoup their losses from fraudulent transfers or outright theft through the app, despite federal regulations intended to prevent and remedy precisely such damages.²⁰ The office of Massachusetts Senator Elizabeth Warren recently released a report on these problems,²¹ noting that banks, by law, are required to make customers whole when they experience losses through unauthorized transfers. The Consumer Financial Protection Bureau (CFPB) is charged with the enforcement of “Regulation E,” a federal rule dating back to 1978, which requires banks to reimburse customers for losses incurred through fraud.²² Senator Warren found rampant noncompliance with Regulation E on the part of banks that market and use the Zelle payment app; her report notes that among banks that responded to her queries, only 47 percent of the amounts reported stolen were returned to customers.²¹ This figure is especially troubling in light of the finding that an estimated \$440 million in assets were lost through Zelle-based frauds and scams in 2021 alone.²¹

Many scammers also target or use cryptocurrencies such as Bitcoin. The technology for forging checks and other financial instruments is increasingly sophisticated; thieves can quickly alter details on a check using electronic tools that render the document nearly indistinguishable from an original in the victim’s own handwriting. Some of these schemes involve persons stealing bill payments from victims’ mailboxes and altering key details on the check, or using the bank’s routing number and account number from the check, to initiate fraudulent transfers. Finally, a variety of newer apps and websites, such as Robinhood, facilitate participation in stock market trading, and adults (not merely vulnerable older adults, but all adults) can lose substantial sums of

money in very little time through risky investments and imprudent trades. In one tragic case, the family of a 20-year-old man who died by suicide after losing a large amount of money through Robinhood (and erroneously believing that he had incurred a large amount of debt) sued and settled with the company for wrongful death and negligent infliction of emotional distress.²³

Further risks are posed by unprecedented advances in artificial intelligence (AI) and related technologies, such as deepfakes. In the near future, scammers will likely be able to create sophisticated videos and interactive text conversations that simulate a specific person's mannerisms and personality so convincingly that even that person's closest relatives may be fooled. Deepfake videos, for example, could potentially be generated using audio and video data freely shared through social media apps like TikTok to add sophistication and convincing realism to impersonation cons, such as grandparent scams or government official imposter schemes. AI today can already be trained to learn and deploy the variables of a specific individual's voice and writing style to generate new text or audio that is indistinguishable from original material written by that person. Such advances will make e-mail phishing attempts far more convincing.

Data analytics and data brokers represent another potential threat to Americans' financial security. Some analytics firms participate in black market or "gray market" forums wherein personal data gleaned through consumer marketing research and the use of apps and other technologies are sold, sometimes to buyers intending to use the data for identity theft. Demographic and personally identifiable information held by data brokers may also be used by scammers to locate and target individuals most likely to be susceptible to financial exploitation. The practice of "friending" on social networking sites may present similar risks; lonely older adults may accept friend requests from strangers on social media without realizing that these new "friends" are scammers or bot accounts (computer programs with fake human personas) designed to collect personal information that could be sold or used for nefarious purposes in the future.

The Importance of Prevention

Scam Awareness

Familiarity with the common scams that target older adults may be helpful. Among the most prevalent

in recent years are romance scams, grandparent scams, government impersonation scams, charity or lottery scams, tech support scams, phishing, e-mail extortion, cryptocurrency fraud, and overpayment scams.^{5,24} As Zhang and colleagues note, romance scams are the costliest, whereas online shopping scams are the most common.¹ The National Elder Fraud Hotline provides succinct informational briefings on some of these scams, including tips on how to recognize them and avoid them.²⁴ Many of these cons involve EFTs or gift card purchases and an expression of urgency by the scammer, implying that if one does not act quickly, negative consequences could be swift; for example, in grandparent scams, sometimes the fraudster impersonates a grandchild and claims to need money urgently for bail or an important medical bill.⁵ Recent years have seen numerous scams in which perpetrators impersonate officials from government agencies. In one notable case, fraudsters claiming to be from the Office of the Inspector General targeted an older adult to steal more than \$500,000 worth of cryptocurrency by claiming that the funds had been misappropriated and used by drug traffickers and money launderers and that the victim's assets would be frozen.²⁵ There have also been reports of con artists claiming to be from the National Elder Fraud Hotline.²⁶ Mental health professionals treating older adults and other vulnerable persons may find the analysis of romance fraud dynamics by Cross, Dragiewicz, and Richards²⁷ helpful in terms of understanding how such scams are conducted.

Financial Planning and Elder Law Services

In addition to familiarity with common scams, planning for future financial incapacity may be prudent. A good working relationship with an accountant or lawyer who is competent to provide advice on asset management is a sound foundation on which to build a more secure future. Depending on an older adult's financial situation, consulting with an elder law specialist might be advisable. Elder law attorneys can provide advice about asset protection, such as the formation of trusts and advance directives that anticipate future needs in the event of a sudden or gradual loss of capacity to manage one's financial affairs.

Technological Safeguards

Technological tools to increase safety are available. Many financial institutions now offer or even require two-factor authentication. In a now-common iteration

of this safeguard, the bank's software sends a text message with an alphanumeric code to the phone number on record for an account when someone tries to log in to that account. Thus, one's username and password alone are no longer sufficient; one must also possess the phone associated with the account and enter the time-limited code into the website to log in. One drawback to this safeguard is the risk of "SIM swapping," whereby a victim's cell phone number is appropriated by the scammer.

Another option for two-factor authentication that is growing more popular is the use of security keys. A security key is a piece of hardware that has an interactive electronic feature to communicate its identity or validity in response to a query. For example, one may insert the security key into the USB port of a laptop or place the security key near one's phone, and when this form of two-factor authentication is enabled or activated, the user must touch the security key when prompted after entering a username and password. Such hardware can be kept in a fireproof lockbox for safekeeping, and a second key may be given to a trusted party (such as the older adult's attorney or spouse) in the event that the elder misplaces the key, or even as a way of facilitating access to account information by a fiduciary when monitoring the individual's finances becomes necessary.

The software that manages bank and credit card accounts can usually be configured to send an alert to the account owner anytime a charge, withdrawal, or transfer over a certain specified monetary amount occurs. So, for example, one might add a setting to a credit card whereby a text notification would arrive on one's mobile phone when a purchase was made using the card for any amount exceeding \$1,000. Bankers and customer service representatives employed by financial institutions can assist older adults or their legal representatives in establishing such safeguards.

Ethics

Ethics principles are of special importance in helping to mitigate risks. The law seeks to protect an individual's autonomy to the maximum extent possible without sacrificing a person's wellbeing or the safety of others. Zhang *et al.* allude to this important balancing test in their article.¹ As Glezer and Devido²⁸ note in the context of forensic assessments of an individual's capacity to enter into a marriage contract, "[t]he goal is to prevent manipulation of a potentially

impaired or otherwise vulnerable person through exploitative contractual arrangements and to balance respect for autonomy against beneficence and nonmaleficence" (Ref. 28, p 292). The ethics-related risks and benefits of different approaches to financial management for older adults vary according to the individual's past, current, and future expected functional capacity. "Excessive charity" has been identified as a possible manifestation of impulse control dysfunction in Parkinson's disease, for example,²⁹ but the question of what makes a gift or donation excessive is a subjective one. Such determinations must be made in light of the individual's values, personality, and prior expressed preferences. In the context of persons with neurocognitive disorder, relevant ethics concerns may evolve as the disorder progresses.³⁰

Guardianship may be considered in the wake of extensive financial losses resulting from fraud or other forms of digital financial exploitation, but there are alternatives to guardianship that carry varying levels of personal or financial risk and which can help to enhance protection for the older adult without sacrificing as much autonomy as traditional guardianships require.³¹ Read and Spar³² present a brief overview of such options and their corresponding degree of risk, including powers of attorney, bill-paying services, joint tenancy for accounts, durable powers of attorney, the designation of representative payees, establishment of personal trusts, limited guardianships, and plenary guardianships. Springing powers of attorney may help to limit the risk of financial exploitation by an appointed agent.³³ An attorney can assist older adults and their loved ones in establishing such safeguards.

In elder law practice, a common ethics dilemma for attorneys is the question of "who is the client?"³⁴⁻³⁶ Family members concerned about an older loved one's impending or progressing neurocognitive impairment may bring their relative to an attorney requesting assistance with estate planning or other legal matters (or, perhaps, to a psychiatrist seeking a physician's "rubber stamp" on allegations of disabling impairment to justify legal actions with more risk to the elder's autonomy). Nonetheless, if the attorney (or physician) is retained to assist in the financial and legal matters (or medical care) of the older adult, the client is that elderly person and not the adult child who facilitated the office visit. As with psychiatrists' responsibilities first to their patients, the lawyer's fiduciary duty, therefore, is to the older adult. This duty is of essential

importance in the context of financial decision-making, as disagreements about spending and financial decisions between concerned relatives and older adults are common. An adult child may wish to restrict an older parent's spending power to obtain a larger inheritance upon the elder's death; however, the older adult may wish to spend more of their hard-earned assets on enjoyable activities or gift giving before losing the ability to do so. In such cases, undue restriction of an elder's spending power may represent an abuse of the caregiver's power and may constitute a violation of the older adult's civil rights.

Loss of personal autonomy is among the most feared sequelae of advancing age. Consider the following hypothetical clinical vignette:

John Doe calls your office expressing concern about his mother, Jane, who he says has been spending increasing amounts of time on Facebook and other forms of social media. He is especially concerned about the relationship that appears to be developing between his mother and a man whom she refers to as "Bobby." According to Jane, Bobby is a handsome retiree who lives in Australia. Jane and Bobby have not met in person, and John is concerned that his mother may be falling victim to a catfishing romance scam. His concern has heightened in recent months, as his mother has been talking about planning a trip to Australia to visit Bobby in person. Although Jane has been diagnosed with mild cognitive impairment, she is in good physical health and is enthusiastic about traveling. She has declined her son's request to accompany her on this trip, and when John has asked her to introduce him to Bobby through a video call, Bobby always seems to have a convenient excuse for being unavailable. John's concern is heightened when he learns that his mother and Bobby have never had a video call and that all of their contact has occurred through text messages, phone calls, and messages exchanged through Facebook Dating. John calls requesting advice on how to protect his mother (who is your patient) from exploitation and financial losses should Bobby indeed turn out to be a romance scammer.

In such a scenario, the psychiatrist must take care to avoid overreaction or paternalistic bias in favor of the concerned relative. As Sprehe notes, "[t]he first axiom of the psychiatrist who is examining an elderly person for legal purposes should be that advanced age alone does not equate with incompetence" (Ref. 37, p 652). The capacity-screening instruments and other tools described by Zhang *et al.*¹ will assist the mental health professional in ensuring that the evaluation is as thorough and unbiased as possible. Competent adults have the legal right to make financial decisions that may be thought unwise or imprudent by others.

Ethics concerns often arise when an older adult's loved one appears to be financially exploiting them, which is unfortunately a common occurrence.³⁸ If

the potential misappropriation of funds is minor and the person using the funds is a trusted adult child well loved by the parent and central to the parent's psychosocial support network, criminal prosecution or reporting the concern to adult protective services may not be advisable from an ethics perspective, given the importance of close relationships to the vulnerable adult. Intervention through less punitive and more nuanced, collaborative approaches may enable preservation of the elder's financial and emotional assets. Kilaberia and Stum³⁹ describe a successful intervention in this type of case.

Warning Signs

The National Adult Protective Services Association (NAPSA) identifies the following warning signs of elder financial exploitation: unusual financial activity (such as large withdrawals or transfers), missing checks or bank statements, changes to names or addresses on accounts, purchases that the account owner cannot remember making, new authorized signatures, missing personal belongings, changes to a financial power of attorney, and changes in ownership of bank accounts or physical property deeds.⁴⁰ Additional warning signs of financial abuse include unpaid bills or eviction notices, bank statements no longer arriving at home (e.g., recent switch to electronic statements), beneficiary changes, reluctance or inability on the part of the older person to discuss financial matters, excessive caregiver interest in the elder's finances, a caregiver restricting the elder's access to communication with others, new close friendships or romantic relationships, or the appearance of sudden expensive acquisitions on the part of a caregiver.⁵ Such warning signs must be considered within the context of the older adult's prior functioning and current situation, and the analysis should be made on a case-by-case basis. New mistakes by someone who has always managed the household finances should raise more concern for neurocognitive impairment and vulnerability to financial exploitation than the same errors when made by an older adult who was not previously responsible for household money management but who has undertaken such tasks after the death of a partner who handled the finances.⁴¹

When an older adult executes a change in testamentary plans that marks a departure from earlier estate plans (such as amending one's will to disinherit a child), evaluations for testamentary capacity and

possible undue influence may be advisable. Hiring an elder law specialist attorney in such situations can be helpful. The American College of Trust and Estate Counsel (ACTEC)⁴² and the National Academy of Elder Law Attorneys (NAELA)⁴³ provide member lawyers with continuing legal education, including training on common financial risks and strategies to protect assets, prevent losses, and increase the likelihood of asset recovery in the event of future losses, as well as guidance on common ethics concerns in the practice of elder law.

Resources for Prevention and Education

Familiarity with the prevalent scams and trends in technologically facilitated financial exploitation may help to lessen the risk of future victimization. With respect to digital imposter scams, one analysis found that:

There is strong evidence that the inoculation process successfully and significantly increases fraud detection without decreasing trust in real communications. It provides protection against both SSA [Social Security Administration] and non-SSA scams, such as Amazon imposter scams. The impact, however, is specific to the mode of communication (email versus letter or SMS) and decays over time; training programs should be targeted accordingly (Ref. 44, p 1).

Continuing education is likely the most effective strategy. To stay informed about common scams, older adults and their families can sign up for content alerts (such as e-mail newsletters) and educational webinars and multimedia from various government and commerce-oriented organizations and nonprofits, including:

- Advocating Against Romance Scammers⁴⁵
- Better Business Bureau⁴⁶
- Consumer Action⁴⁷
- Federal Bureau of Investigation (FBI)⁴⁸
- Federal Trade Commission (FTC)⁴⁹
- Insurance companies (e.g., life insurance carriers)
- Investor Protection Trust⁵⁰
- National Adult Protective Services Association (NAPSA)⁵¹
- National Center on Elder Abuse⁵²
- National White Collar Crime Center (NW3C)⁵³

Social networking sites and apps such as Facebook, Twitter, and LinkedIn may provide interactive options for learning and staying informed, which may be attractive to older adults who are experiencing loneliness. For example, NAPSA offers monthly scam advice forums and a Google Group for members to network and stay informed. On YouTube, which has interactive social features, one can find educational videos from entities like the FBI

(e.g., news release about a romance scammer who stole more than \$700k from an elderly man).⁵⁴ It bears noting, however, that many scams targeting older adults originate through social media. In one recent set of cases, romance scammers used the social game Words With Friends to identify and pursue vulnerable marks, leading to losses of significantly more than \$100,000 for some victims.⁵⁵ Attorneys and financial planners frequently offer free educational workshops in local communities, such as at senior centers and assisted living facilities, where older adults and their families can learn about different legal tools, such as trusts, that are available to help protect one's financial resources. These educational forums may even provide additional opportunities for socialization and interaction with others in the community.

Although research is needed to confirm this hypothesis, preventive education is likely the most effective strategy to reduce potential future losses from elder digital financial exploitation. Nearly everyone who has an e-mail address has received at least one phishing attempt, and because we are primed to recognize red flags for a scam (such as unusual-looking hyperlinks, urgent requests for wire transfers, or allegations that the sender is Nigerian royalty), many of us hardly even consider such e-mails once we see them in our inboxes. We quickly identify the red flags, and we delete the e-mails accordingly. As the public grows more wary of digital solicitation, however, scammers and fraudsters respond accordingly by increasing the level of sophistication and ingenuity in their schemes. Thus, continuing preventive education will play an essential role in financial risk mitigation.

Resources for Recovery

When losses occur, or when fraud is suspected, there are resources available to older adults and their loved ones. In 2020, the U.S. Department of Justice launched a National Elder Fraud Hotline (1-833-FRAUD-11/1-833-372-8311), which is staffed by social workers, elder services specialists, and victim advocates in financial crimes and exploitation.⁵⁶ The hotline was established to facilitate the reporting of fraud that targets individuals 60 and older. Reporting suspected fraud victimization as early as possible is advisable; the Department of Justice notes that reporting financial losses from such crimes within the first two to three days increases the likelihood of

recouping one's losses.⁵⁷ Fraud victims can also report such incidents to:

- Consumer Financial Protection Bureau (CFPB) (for complaints about financial products)⁵⁸
- Elder Justice Initiative of the U.S. Department of Justice⁵⁹
- Federal Trade Commission (FTC)⁴⁹
- Financial Industry Regulatory Authority (FINRA),⁶⁰ which also has a hotline²
- Internet Crime Complaint Center (IC3)⁶¹ of the FBI, which has a section specifically devoted to Elder Fraud⁶²
- The state Attorney General's consumer protection division

As was noted in this journal in the context of technological risks to children and adolescents, “[f]orensic psychiatrists in the 21st century can expect to encounter technology-related social problems for which existing legal remedies are limited” (Ref. 63, p 322). Changes in the law often lag behind advances in technology, and persons who care for older adults may play an important role in advocating for legislative changes and other mechanisms to protect vulnerable persons from technology-facilitated financial abuse in the future.

Conclusion

The threat posed by digital financial exploitation extends far beyond older adults and their families. Some of the most common scams and frauds have grown so sophisticated that even the most astute and technologically savvy among us are vulnerable, and staggeringly vast amounts of wealth have been lost through such schemes in recent years. Mental health professionals can play a valuable role in educating vulnerable older adults about scams and risks to consider in technologically mediated activities ranging from investment trading and financial affairs management to the use of dating apps and video games.⁶⁴ Given the costly nature of romance scams and the prevalence of online shopping scams, these two types of fraud may represent ideal examples for conversation starters to help patients, evaluatees, and caregivers learn more about how to protect their financial wellbeing in the years to come.

References

1. Zhang T, Morris NP, McNeil DE, Binder R. Elder financial exploitation in the digital age. *J Am Acad Psychiatry Law*. 2023 Jun; 51(2):173–80
2. Edersheim J, Murray ED, Padmanabhan JL, Price BH. Protecting the health and finances of the elderly with early cognitive impairment. *J Am Acad Psychiatry Law*. 2017 Mar; 45(1):81–91
3. Burnes D, Henderson CR, Sheppard C, *et al*. Prevalence of financial fraud and scams among older adults in the United States:

- A systematic review and meta-analysis. *Am J Public Health*. 2017; 107(8):e13–e21
4. Internet Crime Complaint Center (IC3), U.S. Federal Bureau of Investigation. Fraud report 2021. Washington, DC: IC3, FBI; 2022. Available from: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf. Accessed January 5, 2023
 5. Kohn R, Warner J, Verhoek-Oftedahl W, Murphy E. Elder Abuse. In Holzer JC, Kohn R, Ellison JM, Recupero PR, editors. *Geriatric Forensic Psychiatry: Principles and Practice*. New York: Oxford University Press, 2016. p. 171–80
 6. Jackson SL. A systematic review of financial exploitation measures in prevalence studies. *J Appl Gerontol*. 2018; 37(9):1150–88
 7. Tyler ET. Socially Vulnerable Older Adults & Medical-Legal Partnership. Washington, DC: National Center for Medical-Legal Partnership at The George Washington University; 2019. Available from: <https://medical-legalpartnership.org/wp-content/uploads/2019/03/Socially-Vulnerable-Older-Adults-and-MLP.pdf>. Accessed February 5, 2023
 8. Frolik LA, Kaplan RL. Introduction: The scope and diversity of elder law. In Frolik LA, Kaplan RL, editors. *Elder Law in a Nutshell*, Fifth Edition. St. Paul, MN: West Publishing Co; 2010. p. 1–7
 9. Beach SR, Schulz R, Sneed R. Associations between social support, social networks, and financial exploitation in older adults. *J Appl Gerontol*. 2018; 37(8):990–1011
 10. DeLiema M. Elder fraud and financial exploitation: Application of routine activity theory. *Gerontologist*. 2018; 58(4):706–18
 11. Goldstein D, Gebeloff R. As Gen X and boomers age, they confront living alone. *The New York Times* [Internet]; 2022 Nov 27. Available from: <https://www.nytimes.com/2022/11/27/us/living-alone-aging.html>. Accessed December 8, 2022
 12. MetLife. *TheMetLife study of elder financial abuse: Crimes of occasion, desperation, and predation against America's elders*. New York: MetLife Mature Market Institute, National Committee for the Prevention of Elder Abuse, and Center for Gerontology at Virginia Polytechnic Institute and State University; 2011. Available from: <https://ltombudsman.org/uploads/files/issues/mmi-elder-financial-abuse.pdf>. Accessed February 5, 2023
 13. Wood SA, Liu PJ, Hanoch Y, Estevez-Cores S. Importance of numeracy as a risk factor for elder financial exploitation in a community sample. *J Gerontol B Psychol Sci Soc Sci*. 2016; 71(6):978–86
 14. Teaster PB, Roberto KA, Savla J, *et al*. Financial fraud of older adults during the early months of the COVID-19 pandemic. *Gerontologist*. 2022. Available from: <http://dx.doi.org/10.1093/geront/gnac188>. Accessed May 23, 2023
 15. National Adult Protective Services Association. *Elder financial exploitation*. Washington, DC: NAPSA; 2017. Available from: <https://www.napsa-now.org/financial-exploitation/>. Accessed January 5, 2023
 16. Knight BG, Kim S, Rastegar S, *et al*. Influences on the perception of elder financial abuse among older adults in southern California. *Int Psychogeriatr*. 2016; 28(1):163–9
 17. Dominguez SF, Ozguler B, Storey JE, Rogers M. Elder abuse vulnerability and risk factors: Is financial abuse different from other subtypes? *J Appl Gerontol*. 2022; 41(4):928–39
 18. National Adult Protective Services Association. *Zelle peer-to-peer payment fraud (NAPSA Scam Forum)*. Washington, DC: NAPSA; 2022 Oct 27. Available from: <https://www.napsa-now.org/wp-content/uploads/2022/11/Baker-Deem-NAPSA-Zelle-Fraud-Resources-OCT-2022.pdf>. Accessed January 5, 2023
 19. Cowley S, Nguyen L. Fraud is flourishing on Zelle. The banks say it's not their problem. *The New York Times* [Internet]; 2022 March 6. Available from: <https://www.nytimes.com/2022/03/06/>

- business/payments-fraud-zelle-banks.html. Accessed January 30, 2023
20. Cowley S. Few customers get refunds for “rampant” Zelle fraud, senator’s report says. *The New York Times* [Internet]; 2022 Oct 3. Available from: <https://www.nytimes.com/2022/10/03/business/zelle-fraud-warren.html>. Accessed January 5, 2023
 21. Office of U.S. Senator Elizabeth Warren. Facilitating fraud: How consumers defrauded on Zelle are left high and dry by the banks that created it. Boston: Office of Sen. Warren; October 2022. Available from: <https://www.warren.senate.gov/download/zelle-report-october-2022>. Accessed January 30, 2023
 22. Cowley S, Nguyen L. When customers say their money was stolen on Zelle, banks often refuse to pay. *The New York Times* [Internet]; 2022 June 20. Available from: <https://www.nytimes.com/2022/06/20/business/zelle-money-stolen-banks.html>. Accessed January 30, 2023
 23. Egan M. Robinhood settles lawsuit over 20-year-old trader who died by suicide. *CNN.com*. 2021 July 1. Available from: <https://www.cnn.com/2021/07/01/business/robinhood-lawsuit-suicide-settlement/index.html>. Accessed January 20, 2023
 24. National Elder Fraud Hotline, U.S. Department of Justice, Office for Victim of Crime. Common scams and warning signs. Washington, DC: U.S. DOJ OVC, National Elder Fraud Hotline; 2022. Available from: <https://ovc.ojp.gov/program/stop-elder-fraud/common-scams-and-warning-signs>. Accessed January 5, 2023
 25. United States Attorney’s Office, Western District of North Carolina. U.S. Attorney Dena J. King announces the successful forfeiture and return of stolen cryptocurrency to elderly man victimized by government imposter scam. Asheville, NC: USAO, W.D. N.C.; March 15 2022. Available from: <https://www.justice.gov/usao-wdnc/pr/us-attorney-dena-j-king-announces-successful-forfeiture-and-return-stolen>. Accessed January 5, 2023
 26. US. Department Of Justice Office for Victims of Crime. Fraud alert: National Elder Fraud Hotline impersonation scams. Washington, DC: U.S. DOJ OVC; 2022. Available from: <https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope#fraud-alert-national-elder-fraud-hotline-impersonation-scams>. Accessed January 5, 2023
 27. Cross C, Dragiewicz M, Richards K. Understanding romance fraud: Insights from domestic violence research. *Brit J Criminology*. 2018; 58(6):1303–22
 28. Glezer A, Devido JJ. Evaluation of the capacity to marry. *J Am Acad Psychiatry Law*. 2017 Sep; 45(3):292–7
 29. El Otmani H, Abdulkhakeem Z, El Moutawakil B, *et al*. Excessive charity: A new aspect of impulse control disorders in Parkinson’s disease. *Int Psychogeriatr*. 2020; 32(5):665–6
 30. Johnson RA, Karlawish J. A review of ethical issues in dementia. *Int Psychogeriatr*. 2015; 27(10):1635–47
 31. Arias JJ. A time to step in: Legal mechanisms for protecting those with declining capacity. *Am J L & Med*. 2013; 39(1):134–59
 32. Read SL, Spar JE. Capacity, informed consent, and guardianship. In Holzer JC, Kohn R, Ellison JM, Recupero PR, editors. *Geriatric Forensic Psychiatry: Principles and Practice*. New York: Oxford University Press; 2016. p. 75–81
 33. Craft JC. Preventing exploitation and preserving autonomy: Making springing powers of attorney the standard. *U Balt L Rev*. 2015; 44:407–67
 34. Brashier RC. The professional responsibilities of the lawyer. In Brashier RC, editor. *Mastering Elder Law*. Durham, NC: Carolina Academic Press; 2010. p. 445–66
 35. Recupero PR. The role of law and the legal profession and relationship to the psychiatric consultant. In Holzer JC, Kohn R, Ellison JM, Recupero PR, editors. *Geriatric Forensic Psychiatry: Principles and Practice*. New York: Oxford University Press; 2016. p. 337–42
 36. Brake GB. Ethical issues in dealing with families of elderly clients. *J Legal Prof*. 2005/2006; 30:103–15
 37. Sprehe DJ. Geriatric psychiatry and the law. In Rosner R, editor. *Principles & Practice of Forensic Psychiatry*, 2nd Edition. Boca Raton, FL: Taylor & Francis; 2003. p. 651–60
 38. Chan ACY, Stum MS. A family systems perspective of elder family financial exploitation: Examining family context profiles. *J Appl Gerontol*. 2022; 41(4):945–51
 39. Kilaberia TR, Stum MS. Successful family-driven intervention in elder family financial exploitation: A case study. *Gerontologist*. 2022; 62(7):1029–37
 40. National Adult Protective Services Association. Learning about financial exploitation. Washington, DC: NAPSA; 2023. Available from: <https://www.napsa-now.org/financial-exploitation/>. Accessed January 5, 2023
 41. Frakey LL, Davidoff DA. Neuropsychological assessment in geriatric forensic psychiatry. In Holzer JC, Kohn R, Ellison JM, Recupero PR, editors. *Geriatric Forensic Psychiatry: Principles and Practice*. New York: Oxford University Press; 2016. p. 27–40
 42. American College of Trust and Estate Counsel. Description of the college [Internet]; 2023. Available from: <https://www.actec.org/about-us/>. Accessed February 24, 2023
 43. National Academy of Elder Law Attorneys. About NAELA [Internet]; 2023. Available from: https://www.naela.org/Web/ImportTemp/About_NAELA_New.aspx. Accessed February 24, 2023
 44. Robb CA, Wendel S. Who can you trust? Assessing vulnerability to digital imposter scams. *J Consum Policy*. 2023; 46(1):27–51
 45. Advocating Against Romance Scammers. AARS homepage [Internet]; 2023. Available from: <https://advocatingforu.com>. Accessed February 24, 2023
 46. Better Business Bureau. BBB homepage [Internet]; 2023. Available from: <https://www.bbb.org/>. Accessed February 24, 2023
 47. Consumer Action. Welcome to Consumer Action [Internet]; 2023. Available from: <https://www.consumer-action.org/>. Accessed February 24, 2023
 48. Federal Bureau of Investigation. What we investigate: White-collar crime [Internet]; 2023. Available from: <https://www.fbi.gov/investigate/white-collar-crime>. Accessed February 24, 2023
 49. Federal Trade Commission. FTC homepage [Internet]; 2023. Available from: <https://www.ftc.gov/>. Accessed February 24, 2023
 50. Investor Protection Trust. Devoted to providing unbiased investor education and funding investor protection efforts [Internet]; 2023. Available from: <https://investorprotection.org/>. Accessed February 24, 2023
 51. National Adult Protective Services Association. NAPSA homepage [Internet]; 2023. Available from: <https://www.napsa-now.org/>. Accessed February 24, 2023
 52. U.S. Department of Health and Human Services, Administration for Community Living, National Center on Elder Abuse [Internet]; 2023. Available from: <https://ncea.acl.gov/>. Accessed February 24, 2023
 53. National White Collar Crime Center. NW3C homepage [Internet]; 2023. Available from: <https://www.nw3c.org/>. Accessed February 24, 2023
 54. U.S. Federal Bureau of Investigation. How a romance scammer stole over \$700,000. Baltimore, MD: U.S. FBI; 2022 Feb 11. Available from: <https://www.youtube.com/watch?v=lxReHY2SBwv>. Accessed January 16, 2023
 55. Rohde M. When Words With Friends turns ugly. *AARP.com* [Internet]; 2020 Oct 2. Available from: <https://www.aarp.org/money/scams-fraud/info-2020/words-with-friends-romance-scam.html>. Accessed January 20, 2023
 56. U.S. Department of Justice, Office of the Attorney General. Annual report to Congress on Department of Justice activities to combat elder fraud and abuse. Washington, DC: United States DOJ,

Recupero

- OAG; 2022 Oct 18. Available from: <https://www.justice.gov/file/1544891/download>. Accessed January 30, 2023
57. U.S. Department of Justice, Office of Public Affairs. Fraud alert: Scammers claiming to be with DOJ, preying on elderly. Washington, DC: U.S. DOJ OPA; 2020 Sep 4. Available from: <https://www.justice.gov/opa/pr/fraud-alert-scammers-claiming-be-doj-preying-elderly>. Accessed January 5, 2023
 58. Consumer Financial Protection Bureau. Submit a complaint about a financial product or service [Internet]; 2023. Available from: <https://www.consumerfinance.gov/complaint/>. Accessed February 24, 2023
 59. U.S. Department of Justice. Elder Justice Initiative (EJI) [Internet]; 2023. Available from: <https://www.justice.gov/elderjustice>. Accessed February 24 2023
 60. Financial Industry Regulatory Authority. FINRA homepage [Internet]; 2023. Available from: <https://www.finra.org/>. Accessed February 24, 2023
 61. U.S. Federal Bureau of Investigation. Internet Crime Complaint Center (IC3) [Internet]; 2023. Available from: <https://www.ic3.gov/>. Accessed February 24, 2023
 62. U.S. Federal Bureau of Investigation, IC3. Elder fraud [Internet]; 2023. Available from: <https://www.ic3.gov/Home/EF>. Accessed February 24, 2023
 63. Recupero PR. New technologies, new problems, new laws. *J Am Acad Psychiatry Law*. 2016 Sep; 44(3):322–7
 64. Hategan A, Bourgeois JA, Parthasarathi U, Ambrosini DL. Counseling geriatric patients about opportunity and risk when “digital dating.” *Current Psychiatry*. 2016 Jul; 15(7):74–7