Insights: Financial Capability

February 2025

Authors:

Marguerite DeLiema, PhD
University of Minnesota
School of Social Work

Siyu Gao, MSW
University of Minnesota
School of Social Work

Daniel Brannock, MS
RTI International

Lynn Langton, PhD
RTI International

Olivia Valdes, PhD
FINRA Investor
Education Foundation

Table of Contents

The issue brief summarizes the findings from the paper *"The effects of risky behaviors and social factors on the frequency of fraud victimization among known victims."* The corresponding author for this issue brief and the full paper is Marguerite DeLiema (email address: mdeliema@umn.edu).

Do older adults' "routine activities" increase fraud risk?

An analysis of the factors that might affect the risk of fraud victimization

Summary

Though financial fraud is widespread and its consequences detrimental to adults across the age spectrum, some criminals specifically target older adults. Understanding which social and behavioral factors are tied to fraud victimization can help identify and protect potential victims from losing money. In this brief, we use survey data from 905 known fraud victims in the United States identified by the U.S. Postal Inspection Service (USPIS) to examine the role of social and behavioral characteristics on victimization experiences. Specifically, we focus on how these factors are associated with the frequency of victimization with any of the following self-reported types of financial fraud in the past year: (1) romance and friend/family imposter scams; (2) charity fraud; (3) investment fraud; (4) product and services fraud; and (5) prize or grant fraud.

We found that engaging in activities that increase fraud exposure—such as opening junk mail, entering sweepstakes drawings to win prizes, answering unknown calls and interacting with telemarketers—was tied to a greater number of different fraud victimization experiences. In addition, older age, loneliness, financial or emotional precarity, and risky financial preferences and behaviors, characteristics that may be perceived as exploitable to fraudsters, were also associated with more forms of fraud victimization. Surprisingly, however, more frequent online activity was tied to fewer fraud victimization experiences, and both social engagement and living with others were unrelated to the number of different forms of fraud victimization experiences.

These findings suggest that interventions should address unmet social and financial needs and that educational efforts are needed to inform vulnerable individuals about reducing risky behaviors that increase fraud exposure.

Background

Mass marketing fraud has a negative impact on adults of all ages, with consequences that include financial, physical and emotional harm, such as poor sleep, loss of trust, shame, embarrassment, reputational costs and loss of financial security (Button et al., 2014; Morgan, 2021). Mass marketing fraud includes scams that target many victims simultaneously using mass communication methods, such as phone, mail, text message, email, social media and other channels. There were 2.6 million cases of fraud reported in 2023, with losses totaling $10 billion (Federal Trade Commission (FTC), 2024), although actual costs may be as high as $137 billion (FTC, 2023). Older adults report significantly greater losses per incident relative to young and middle-aged adults (FTC, 2023).

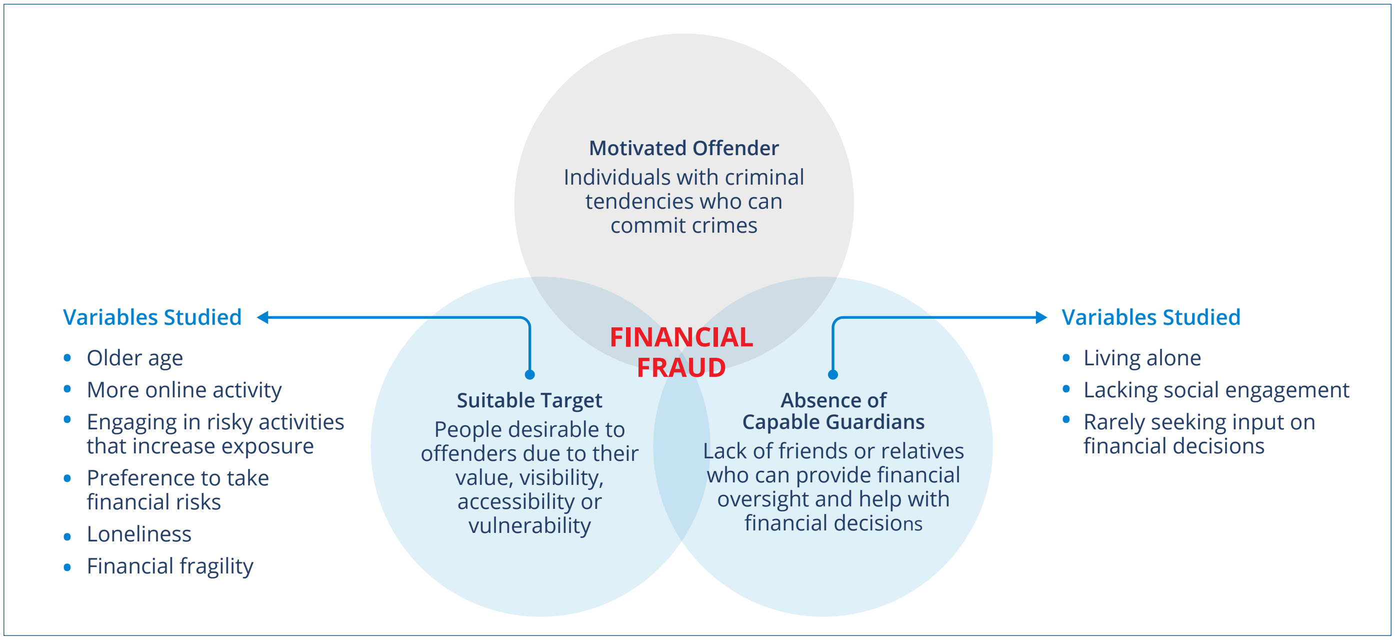
In the present study, we survey known mail fraud victims to better understand their behaviors, financial risk preferences, and social and demographic characteristics. Surveying a known victim population—in this case, a sample of adults predominantly age 60 and older—has the advantage of providing more insight into those who are known to be vulnerable to scams while also addressing limitations cited in other fraud surveys. These limitations include underreporting fraud due to social desirability bias or a lack of acknowledgment of victimization (Beals et al., 2017; Parti & Tahir, 2023).

Routine Activities Theory (RAT)

RAT (Cohen & Felson, 1979) is a framework investigators use to explain shifts in crime patterns in the United States. It emphasizes factors beyond conventional demographic characteristics to explain the likelihood of victimization. Though investigators developed RAT for criminological contexts, such as sexual assault and property crimes, it has been used to describe risk factors for cybercrimes, including identity theft and some forms of fraud and financial abuse. According to RAT, criminal opportunities arise when a *suitable target*—that is, someone or something that may be desirable to perpetrators in terms of perceived value or accessibility—encounters a *motivated offender* or a willing criminal in the *absence of a capable* guardian who can deter or stop the crime from occurring, such as a witness, security system, or physical barrier.

In this brief, we use the RAT framework to examine the role of *suitable targets* and *capable guardians* on the frequency of fraud victimization across five types of fraud. Specifically, we examine characteristics like older age, engagement with risky activities, online activity, preference for financial risk, loneliness and financial fragility—all of which have been previously identified in separate studies as characteristics and behaviors that might make a person a *suitable target* for financial fraud victimization. In addition, we study the potential risks associated with living alone, low frequency of social engagement and rarely seeking input on financial decisions on the frequency of unique forms of fraud victimization. Together, these factors may be conceptualized as the *absence of capable guardians*.

Figure 1. Routine Activity Theory (RAT) Framework: Applications to Financial Fraud



Study Design and Methods

Participants

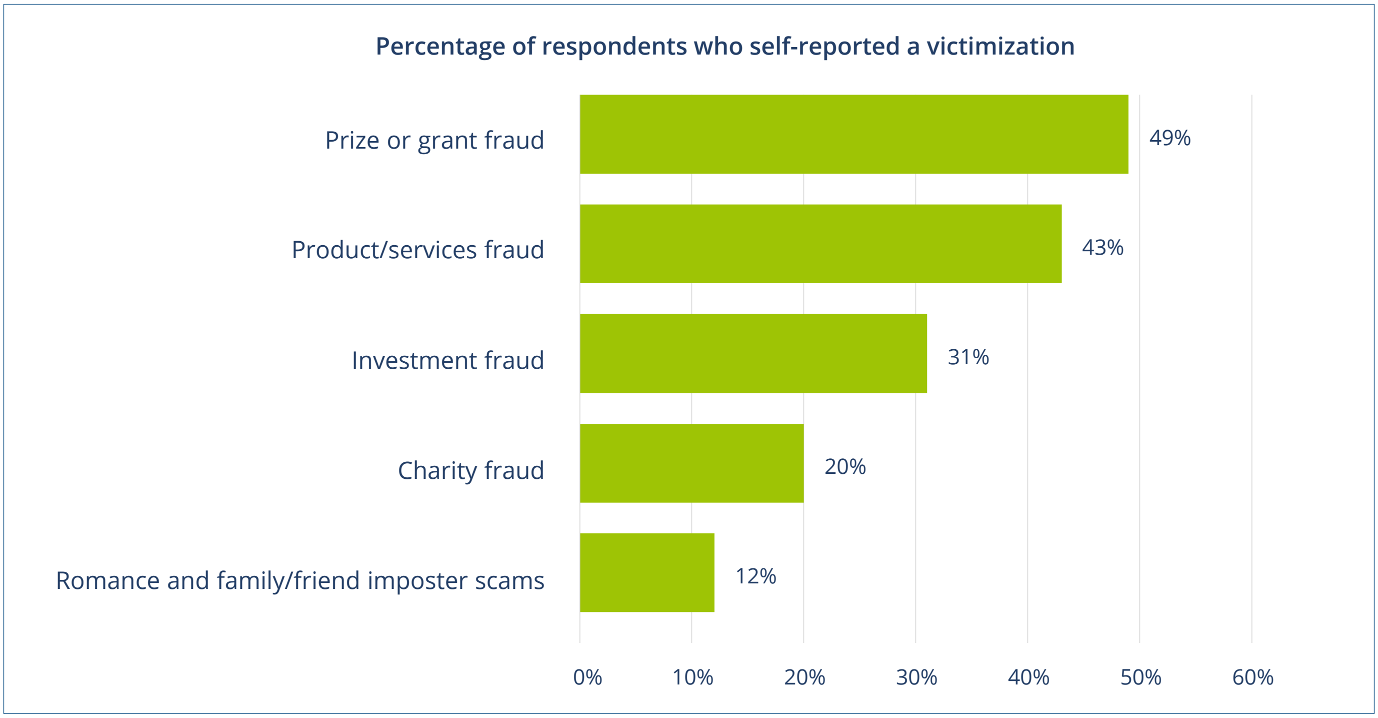
We drew survey data from a sample of mass marketing fraud victims the U.S. Postal Inspection Service (USPIS) identified. The sample included individuals who responded by mail to one or more fraudulent solicitations sent between 2022 and 2023. USPIS identified the victim households and securely provided their addresses to the researchers. We sent survey invitations by mail, but participants could complete the survey online or mail back a completed paper-and-pencil survey. We dropped twenty-nine survey responses due to missing data on fraud victimization in the past year. This resulted in a final sample of 905 respondents.

Study participants were mostly older adults (mean age = 75, standard deviation = 13.2), 46 percent were male, 27 percent were married, 34 percent were widowed and 32 percent had at most completed high school. About one-third of respondents (30 percent) identified as white.

Fraud measure (dependent variable)

Using items adapted from the Bureau of Justice Statistics' Supplemental Fraud Survey (Morgan, 2021), we asked participants if they paid, invested or donated money in the past 12 months in response to five types of mass marketing fraud solicitations. These five scam types primarily involve promises of positive financial opportunities or social rewards. In other words, most were opportunity-based scams versus threat-based scams. Nearly half the participants (49 percent) reported losing money to a prize or grant fraud, 43 percent reported losing money to product/services fraud, 31 percent to investment fraud, 20 percent to charity fraud, and 12 percent to romance and family/friend imposter scams (see Figure 2). For the dependent measure, we combined these scam types into a single measure representing the total number of different types of fraud the respondents experienced. The minimum was 0 (none) and maximum was 5 (all forms) with a mean of 1.5 and a standard deviation (*SD*) of 1.6.

Figure 2. Frequency of Self-Reported Fraud Victimization by Type in the Past Year (N= 905)



Findings

Who are the more "suitable targets"?

According to RAT, individuals who are desirable to offenders due to their value, visibility, accessibility and vulnerability are termed *suitable targets*. Using this definition, we identified several characteristics and behaviors that may make an individual a "suitable target." Using logistic regression, we related the following factors to the number of different forms of fraud victimization reported in the past year (see Figure 3):

1. **Older age:** Even among a largely older adult sample (mean age = 75), age was positively associated with the number of unique fraud victimizations. These findings persisted even after controlling for social and behavioral characteristics.
2. **Risky activities:** Specific activities that we define as "routine activities" for the purposes of applying the RAT framework—such as entering sweepstakes drawings, opening all mail, not hanging up on telemarketers, and answering unknown calls—were associated with more unique fraud victimization incidents. Given that many fraudsters perpetrate scams by telephone and through the mail (FTC, 2023), engaging in these behaviors may pose a risk to individuals by increasing their exposure to scammers.
3. **Financial risk preferences and behaviors:** Preference for higher financial risk and engagement in certain risky financial behaviors, such as playing lottery games, were tied to a greater number of unique victimization incidents. Individuals who hold a preference for risk and engage in these behaviors might be more easily persuaded by "get rich quick" schemes. Scammers exploit this mentality using phantom fixation—activating fantasies of wealth, romance and prestige—as a persuasion tactic.
4. **Loneliness:** Higher levels of loneliness, defined as feelings of social isolation, were tied to more unique incidents of financial fraud victimization. Adults who are lonely have unmet needs for social stimulation, emotional validation and companionship that might increase their susceptibility to fraud. Many scammers actively appeal to these social and psychological states and exploit targets' emotional vulnerability.
5. **Financial fragility:** Those classified as financially fragile, who indicated they would struggle to cover a $2,000 emergency expense, experienced more unique incidents of fraud victimization in the past year, on average, than those who reported being able to cover an unexpected expense. These individuals might have unmet needs for financial security and be drawn to schemes that promise rewarding financial opportunities.
6. **Online activity:** Contrary to our predictions, more regular online activity was associated with *fewer* unique fraud victimization incidents.

Figure 3. Associations with the Number of Unique Fraud Victimization Incidents

Suitable Target	Absence of Capable Guardians	Socio-demographics
^ Older Age	✕ Lives alone	✕ Male
^ Engages in risky activities	✕ Low social engagement	✕ Married
^ Preference for taking financial risks	✕ Rarely seeks input on financial decisions from trusted others	✕ Higher income
^ Lonely		✕ More education
^ Financially fragile		^ Black/African American
˅ More online activity		^ Hispanic/Latino

Statistical significance at the p<.05 level.

^ *Indicates that the variable is significantly tied to a higher number of unique fraud victimization incidents.*

˅ *Indicates that the variable is significantly tied to the lower number of unique fraud victimization incidents.*

✕ *Indicates that the variable is unrelated to the number of unique fraud victimization incidents.*

The presence of capable guardians and seeking input on financial decisions may not reduce risk

RAT proposes that victimization is more likely to occur in unsupervised settings where there is a lack of capable guardians who could prevent or deter crime. Therefore, we predicted that those who live alone, who are less socially engaged, and who less frequently seek input on financial decisions from people they know and trust would report a greater number of unique fraud victimization incidents. Contrary to our expectations, we found that these factors were unrelated to fraud victimization incidents. One explanation is that the frequency of social interaction with friends and family members is less important than the *quality* of these relationships in preventing fraud. For example, research by Liu and colleagues (2017) found that negative social exchanges with close social network members were associated with elder financial exploitation, even after controlling for social network size. Beach et al. (2013) found that larger social networks and lower perceived social support were simultaneously associated with higher risk for elder financial exploitation. We did not assess relationship quality and network size in our study.

Few sociodemographic factors are uniquely tied to fraud victimization

In addition to the variables related to being a suitable target or the absence of capable guardians, we examined the role of sociodemographic factors. When controlling for behavioral and social characteristics, few demographic factors were associated with the number of unique fraud victimization incidents—with notable exceptions being age and race/ethnicity. We found that Black/African American and Hispanic/Latino respondents reported a higher number of unique fraud incidents than their white counterparts.

Discussion

Overall, our findings partially support RAT as a conceptual framework for fraud victimization. Characteristics and behaviors that might increase one's suitability as a target were mostly tied to greater fraud victimization. Specifically, being older, engaging in risky routine activities, lottery-playing, preferences for financial risk, loneliness, and financial fragility are each associated with a greater number of unique fraud victimizations like prize and grant fraud, charity fraud, imposter scams, and other mass marketing schemes. Contrary to other research (*e.g.*, Gainsbury et al., 2019; Holtfreter et al., 2008; Saridakis et al., 2016; Van Wilsem, 2011), however, we found that engaging in more regular online activity (*e.g.*, active internet use, online shopping and social media use) was associated with a lower number of unique fraud victimization incidents among the sample we studied. Further research is needed to understand the conditions under which online activity decreases versus increases fraud risk, and which types of fraud are associated with online activities. For example, frequent online activity might be associated with exposure to phishing scams and online shopping scams, which were not directly measured in this study.

We find less support for the role of capable guardians as deterrents against fraud victimization. Unlike the theoretical framework of RAT, the absence of capable guardians was unrelated to the number of victimization incidents. Living alone and being less socially engaged were not risk factors; however, loneliness—a subjective measure of social isolation—was a risk factor. Results suggest that while some aspects of RAT—particularly those related to the target's attractiveness to a perpetrator—are supported, the potentially protective role of social and supervisory factors may be more complex than initially hypothesized and warrants further study. Further, it is noteworthy that because respondents were known victims of mass marketing scams, which were perpetrated via mail, their characteristics and factors that are tied to the fraud susceptibility of these individuals may not be representative of those of fraud victims more broadly, thus furthering the need for more studies.

Implications for consumer education

Survey results indicate that certain factors might make individuals more susceptible to financial predators who use persuasive messages promising to address unmet needs. Consumer education programs may want to focus on certain risk factors and characteristics, as scammers often exploit these vulnerabilities with promises of financial gain, social connection or emotional support.

Areas of opportunity for fraud prevention education and intervention programs

Address loneliness: Increasing social engagement through meaningful activities may reduce loneliness, and accordingly reduce vulnerability to scams. Programs that enable older individuals to participate in community events and develop interpersonal relationships could reduce the appeal of many forms of fraud that prey on the need for companionship or inclusion.

Enhance financial knowledge: Teach individuals, especially older adults, how to make informed financial decisions and identify scam messages. Addressing reward-seeking and reduced sensitivity to financial risk is difficult but may be possible through tailored financial literacy programs (*e.g.*, Anderson, 2016; Drew & Cross, 2013).

Assist with money management: Banks and local non-profits may offer free or low-cost services to help older persons with budgeting, expense and debt management, and financial emergency preparation. Offering information about these services or providing monthly financial statement reviews can help older adults better understand their financial circumstances and protect their accounts (*e.g.*, see "SAFE" intervention in Hall et al., 2022).

Target messages to those engaging in risky financial behaviors: Given that purchasing lottery or scratch-off tickets is closely associated with financial fraud incidents, incorporating consumer fraud education into locations where lottery tickets are sold might help in reaching older persons who participate in these games. Educational efforts should teach consumers how to distinguish between legitimate and fake lotteries and sweepstakes and highlight the risks of entering competitions and prize drawings, particularly those that involve an upfront fee or that collect personal information.

Provide education to reduce exposure to pitches: Provide information and education about the risks that behaviors such as answering unknown calls and opening marketing mail pose to increasing scam exposure. Educate consumers on how to take action to reduce their exposure, including:

- **Blocking unwanted calls:** Provide information on how to block unwanted calls or only allow calls from known or approved contacts.
- **Declining telemarketing offers:** Provide scripts and strategies for quickly identifying and hanging up on telemarketers.
- **Managing junk mail:** Educate consumers on the importance of discarding unsolicited mail and recognizing the signs of fraudulent marketing materials.

Acknowledgments

The FINRA Investor Education Foundation provided funding for data analysis and manuscript development. The National Institute of Justice, Office of Justice Programs, U.S. Department of Justice Award No. 2019-R2-CX-0053 provided funding to develop the survey and collect data. The opinions, findings and conclusions expressed in the brief are those of the authors and do not necessarily reflect those of FINRA, the FINRA Investor Education Foundation, the Department of Justice, USPIS or Postal Inspection Service, or any other government agency.

References

Anderson, K. B. (2016). Mass-market consumer fraud: who is most susceptible to becoming a victim?. FTC Bureau of Economics. No. 332, Available at SSRN: https://ssrn.com/abstract=2841286 or http://dx.doi.org/10.2139/ssrn.2841286.

Beals, M. E., Carr, D. C., Mottola, G. R., Deevy, M. J., & Carstensen, L. L. (2017). How does survey context impact self-reported fraud victimization? The Gerontologist, 57(2), 329-340.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27, 36-54.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. Crime: Critical Concepts in Sociology, 1, 316.

Drew, J. M., & Cross, C. (2013). Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes. Journal of Financial Services Marketing, 18, 188-198.

Federal Trade Commission. (2023). Protecting Older Consumers. 2022-2023. Available at https://www.ftc.gov/system/files/ftc_gov/pdf/p144400olderadultsreportoct2023.pdf.

Federal Trade Commission. (2024, February 7). Nationwide fraud losses top $10 billion in 2023 as FTC steps up efforts to protect the public. Available at https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public.

Gainsbury, S. M., Browne, M., & Rockloff, M. (2019). Identifying risky Internet use: Associating negative online experience with specific online behaviours. New Media & Society, 21(6), 1232-1252.

Hall, L., Moray, J., Gross, E., & Lichtenberg, P. A. (2022). Financial stressors and resources associated with financial exploitation. Innovation in Aging, 6(2), igac010.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. Criminology, 46(1), 189-220.

Liu, P. J., Wood, S., Xi, P., Berger, D. E., & Wilber, K. (2017). The role of social support in elder financial exploitation using a community sample. Innovation in aging, 1(1), igx016.

Morgan, R. E. (2021). Financial fraud in the United States, 2017. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Available at: https://bjs.ojp.gov/content/pub/pdf/ffus17.pdf.

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

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. Technological Forecasting and Social Change, 102, 320-330.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. European Journal of Criminology, 8(2), 115-127.

1700 K Street, NW
Washington, DC 20006-1506
www.finrafoundation.org

H27376—02/2025