FINRA Investor Education FOUNDATION

Insights: Financial Capability

November 2022

Authors:

Marguerite DeLiema, Ph.D.
University of Minnesota
School of Social Work

Yiting Li, M.A.
University of Minnesota
Department of Family Social Sciences

Morgan K. Taylor, M.A.
Duke University
Department of Psychology and Neuroscience

Gary R. Mottola, Ph.D.
FINRA Investor Education Foundation

What's Inside

This issue brief summarizes the findings from the paper "Correlates of Responding to and Becoming Victimized by Fraud: Examining Risk Factors by Scam Type" published in the International Journal of Consumer Studies. The corresponding author for this issue brief and the full manuscript is Marguerite DeLiema (mdeliema@umn.edu).

University of Minnesota

Does One Size Fit All? An Examination of Risk Factors by Scam Type

Summary

Using survey data from 1,375 U.S. and Canadian consumers who reported a scam to the Better Business Bureau's (BBB) Scam Tracker website, this study examines the factors related to both responding to and losing money to four types of consumer fraud: (1) opportunity-based scams, (2) threat-based scams, (3) consumer purchase scams, and (4) phishing scams.

We found that risk factors for responding to and losing money to a scam generally varied across scam types, but some patterns did emerge. Specifically, three risk factors were common to most scam types: lacking prior knowledge of the scam, loneliness, and believing the fraudster/organization seemed "official" were tied to a higher risk of responding and/or losing money to the scam. Overall, these findings suggest that educating consumers about specific scams and scammer tactics may be effective at protecting against victimization from a range of fraudulent schemes.

Background

Consumer fraud takes many forms and results in billions of dollars in annual losses. A national study in the United States found that nearly 16 percent of consumers lose money to scams each year (Anderson, 2019), though this figure may under-estimate victimization because many incidents are never reported to authorities or acknowledged by victims in surveys (Anderson, 2021; DeLiema, Shadel, & Pak, 2020; Raval, 2020). In fact, one estimate puts fraud losses at about $50 billion a year in the U.S. alone (Deevy & Beals, 2013).

Using a survey of U.S. and Canadian consumers who reported incidents of financial fraud attempts and victimization to BBB's Scam Tracker website (N=1,375), we examined the demographic, psychological, and contextual factors associated with responding to and losing money in a scam. This is one of few U.S studies to survey individuals who previously filed a fraud report with a consumer protection organization. The advantage of surveying this population is twofold. First, we ensure all participants assessed were targeted by fraud and reported the scam, which reduces survey error caused by individuals under-acknowledging victimization experiences or including participants who have not been targeted by fraud. Second, because the website allows people to report a range of different scams, we can use this information to assess risk factors by scam type: (1) opportunity-based, (2) threat-based, (3) consumer purchase, and (4) phishing scams. Table 1 defines these four types of scams and provides examples. In this brief, we examine how risk factors for victimization vary by scam type and whether there are consistent characteristics that offer promising opportunities for consumer protection and education.

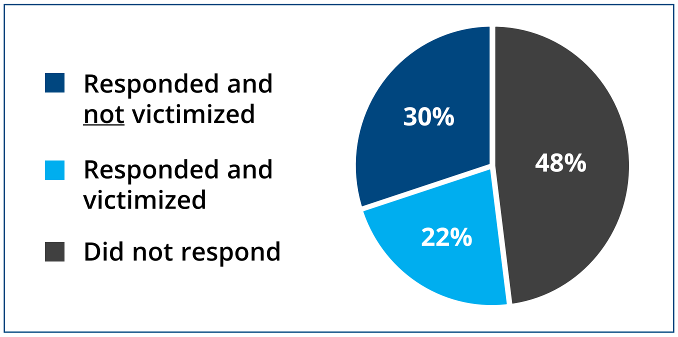
Table 1. Definitions and examples of scam types

Scam Type	Definition	Examples of Fraud Schemes
Opportunity-based scams	Scammers promise something positive and rewarding	Investment scams, bogus sweepstakes/lottery/prizes, fake employment, government grant, advance fee loan, fake check, debt consolidation, secret shopper, and sweetheart/romance scams
Threat-based scams	Scammers say something bad has happened and demand you pay money to avoid negative consequences	Bogus tax collection, government impostor, debt collection, tech support, grandparent scam, extortion, and unnecessary home repair
Consumer purchase scams	Scammers offer products and/or services that do not exist or that are intentionally misrepresented	Online marketplace fraud, pet adoption, health insurance enrollment, bogus charities, and other general consumer scams like billing for non-existent subscriptions
Phishing scams	Scammers impersonate a trustworthy party using email, websites, or text messages to obtain an individual's personal information	Any fraudulent communication that mimics well-known people or organizations (*e.g.*, financial institutions, Amazon), uses professional titles and insignias (*e.g.*, "Special Agent," "Financial Accounts Manager"), and/or presents other indicators of legitimacy to appear trustworthy

Findings

The most frequently reported scams were threat/fear-based (39.9 percent), followed by opportunity-based scams (27.5 percent), consumer purchase scams (16.1 percent) and phishing scams (14.2 percent). Roughly 650 participants did not respond to the scam when they were solicited. That is, they hung up the phone, deleted the email, or otherwise ignored the solicitation, but still reported the experience to BBB Scam Tracker. Among the 719 who did respond to the scam, 307 reported being victimized, meaning they responded and lost money (Figure 1). The median amount of money lost across all scam types was $650.

Figure 1. Response to scams and victimization



Who's most at risk? Depends on the scam

Opportunity-based Scams

Responded

Survey participants with higher levels of loneliness were more likely to respond to opportunity-based scams than those who did not report being lonely, as were participants who lost money in prior scams. Participants who had heard about the specific scam before were less likely to respond.

Lost Money

Males, participants earning higher incomes, those reporting financial fragility (that is, reporting they could not come up with $2,000 in 30 days in the event of a financial emergency), and college-educated participants were more likely to lose money in these scams than their female, lower-income, non-financially fragile, and non-college-educated counterparts. Additionally, believing the fraudster/organization seemed official and choosing not to discuss the fraudulent offer with anyone were each tied to losing money to opportunity-based scams. On the other hand, married participants, those who had previously heard about the scam, and those with higher financial literacy were less likely to lose money to this type of scam (See Table 2).

Threat-based Scams

Responded

Financial fragility and having previously heard about the scam were each tied to lower likelihood of responding to threat-based scams. Loneliness was associated with a higher probability of responding to the fraudulent offer.

Lost Money

Reporting that the fraudster/organization seemed official, having higher levels of loneliness, and/or self-reporting high financial competence (that is, perceiving they were good at dealing with day-to-day financial matters, such as checking accounts, credit and debit cards, and tracking expenses) were tied to losing money to threat-based scams. And participants who did not have anyone to discuss the offer with were also more likely to lose money. Participants who had heard about the scam before being exposed were less likely to lose money, as were those with high financial literacy.

Consumer Purchase Scams

Responded

Like findings for the other scam types, participants who heard about the consumer purchase scam before being exposed were less likely to respond than those who had not heard about the scam.

Lost Money

Higher levels of loneliness, reporting that the fraudster/organization seemed official, and having no one to talk to about the solicitation were each associated with losing money to consumer purchase scams. On the other hand, having someone who tried to intervene to prevent the scam from happening was tied to a lower likelihood of losing money to these types of scams.

Phishing Scams

Identifying as white, non-Hispanic, having attended college, and having previously heard about the scam were each tied to a lower likelihood of responding to phishing scams; however, due to the small number of participants reporting that they lost money in phishing scams (n=6), we could not assess the factors related to victimization.

Table 2. Summary of findings

	Opportunity-Based Scams		Threat-Based Scams		Consumer Purchase Scams	
Risk Factors	Respond	Lose Money	Respond	Lose Money	Respond	Lose Money
Demographic						
Men		More Likely				
Married		Less Likely				
Some College or College Degree		More Likely				
Higher Income		More Likely				
Financially Fragile		More Likely	Less Likely			
Contextual						
Heard about the Scam Before	Less Likely	Less Likely	Less Likely	Less Likely	Less Likely	
Thought Fraudster Seemed “Official”*		More Likely		More Likely		More Likely
Didn’t Have Anyone to Discuss the Scam With*				More Likely		More Likely
Chose Not to Discuss Scam with Anyone*		More Likely				
Someone Tried to Intervene*						Less Likely
Prior Scam Victim	More Likely					
Psychological						
High Financial Literacy		Less Likely		Less Likely		
High Self-Rated Financial Competence				More Likely		
Lonely	More Likely		More Likely	More Likely		More Likely

* Only participants who responded to the scam were asked this question

Responding vs. Losing Money

Risk factors for engaging with a scam can differ from those tied to losing money to it—even for the same scam type. For example, loneliness was associated with responding to opportunity-based scams but not losing money to them. Why? One possible explanation is that opportunity-based scams may be particularly effective at getting people who feel isolated to respond. However, once the consumer engages, loneliness may not further increase their risk of financial loss.

Why do the risk factors differ by scam type?

Previous research has found that people's susceptibility to scams can differ depending on their financial and psychological characteristics, as well as the context in which they were solicited. The products and services that scammers promise and the elements of persuasion they use are tailored to target certain people. For example, our findings show that higher financial literacy was a protective factor against losing money to opportunity-based scams but not threat-based scams. Understanding financial concepts such as inflation and investing may make people more skeptical of "get rich quick" opportunities, but it may not protect them against scams that use fear to persuade them into providing payment.

Some risk and protective factors ARE one-size-fits-all

One risk factor was associated with all scam types—the appearance that the fraudster/organization seemed "official." The use of authority—or source credibility—is a common persuasion tactic in marketing and is popular among scammers. Research shows that fraudulent communications often mimic or reference well-known people or organizations, use professional titles and insignias, and present other indicators of legitimacy to appear trustworthy. While our survey did not specifically ask participants to describe what made the solicitation seem official, consumers provided comments such as "[He] sounded like a sheriff's deputy and he was threatening me with immediate arrest if I didn't comply," and "The phone ID had said 'Apple' and I had been having trouble with my computer." A protective factor associated with all scam types was prior knowledge about the specific scam. In fact, having advance knowledge of the scam reduced vulnerability by up to 86 percent.

Implications for Consumer Education

The results indicate that the risk factors associated with responding to and losing money to scams vary across the different scam types. This suggests that there is no one-size-fits-all victim profile for which to direct fraud prevention education. To be most effective, consumer education may need to be scam-specific and directed to individuals who have a set of characteristics that make them particularly vulnerable to that type of scam. For example, when informing people about how to detect and resist opportunity-based scams, it may be most impactful to focus on individuals who are financially insecure or in debt, regardless of their income. For phishing scams, it may be most effective to focus on those with lower educational attainment. While there were no significant age differences between responding to a scam and victimization, tailoring the message content and medium of delivery for fraud awareness information to younger and older consumers based on these descriptive differences may be helpful.

Given that victim profiles vary by scam type, the challenge for protection agencies and consumer advocates is determining which scams to prioritize in education and awareness efforts—the most common scams or those that result in the greatest costs to victims? It is also challenging to determine the appropriate channels through which to broadcast information about fraud. While this research did not ask consumers who reported knowing about the scam how or where they learned this information, prior research has found the most common sources of fraud awareness are typically news stories and word of mouth (DeLiema et al., 2019).

Efforts to delegitimize scam solicitations so that targets do not perceive them as official are much more difficult. Scammers use a variety of tactics to make their communications seem valid, including many of the same marketing and persuasion tools used in the legitimate consumer marketplace. One important way to inoculate consumers against these techniques is to educate people on the elements of persuasion and encourage them to ask questions and interrogate marketing claims before making a purchase or payment decision (*e.g.*, researching the offer using independent sources).

Acknowledgements

This study would not have been possible without the contributions of Melissa “Mel” Trumpower and Rubens Pessanha from the BBB Institute for Marketplace Trust, Craig Honick from The Good People Research Company, and Emma Fletcher. The authors thank Christine Kieffer, Robert Mascio, and Olivia Valdes for their insightful comments on early drafts of the brief, Donna Hemans for editing the brief, and Shari Crawford and Gina Santangelo for designing the brief. The authors also thank the FINRA Foundation for funding the research. All results, interpretations, and conclusions expressed are those of the research team alone and do not necessarily represent the views of FINRA, the FINRA Investor Education Foundation, or any of its affiliated companies.

References

Anderson, K. B. (2021). To whom do victims of mass-market consumer fraud complain? Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323

Anderson, K. B. (2019). Mass-market consumer fraud in the United States: A 2017 update. Retrieved from https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf

Deevy, M. & Beals, M. (2013). The scope of the problem: An overview of fraud prevalence measurement. Financial Fraud Research Center. Retrieved from https://longevity.stanford.edu/the-scope-of-the-problem-an-overview-of-fraud-prevalence-measurement

DeLiema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. Journal of Consumer Research, 46(5), 904-914. doi:10.1093/jcr/ucz020

DeLiema, M., Fletcher, E., Kieffer, C. N., Mottola, G., Pessanha, R., & Trumpower, M. (2019). Exposed to scams: What separates victims from non-victims? FINRA Investor Education Foundation, Stanford Center on Longevity and BBB Institute for Marketplace Trust. https://www.bbb.org/ExposedtoScams

Raval, D. (2020). Whose voice do we hear in the marketplace? Evidence from consumer complaining behavior. Marketing Science, 39(1), 168-187.

1735 K Street, NW
Washington, DC 20006-1506
www.finrafoundation.org

CCSD-2771—11/22