Exposed to Scams

WHAT SEPARATES VICTIMS FROM NON-VICTIMS?

FINRA Investor Education FOUNDATION

BBB INSTITUTE for MARKETPLACE TRUST

STANFORD CENTER ON LONGEVITY

SEPTEMBER 2019

Exposed to Scams

WHAT SEPARATES VICTIMS FROM NON-VICTIMS?

AUTHORS

Marti DeLiema, Ph.D.
Stanford Center on Longevity

Emma Fletcher
Federal Trade Commission[1]

Christine N. Kieffer
FINRA Foundation

Gary R. Mottola, Ph.D.
FINRA Foundation

Rubens Pessanha, Ed.D., MBA, PMP, GPHR, SPHR, SHRM-SCP
International Association of Better Business Bureaus, Inc.

Melissa "Mel" Trumpower
BBB Institute for Marketplace Trust

ACKNOWLEDGMENTS

The authors would like to thank Craig Honick of Metro Tribal for his work on survey design and data collection, and Susan Arthur for her comments on earlier drafts of the paper. We would also like to thank the Better Business Bureau for access to data from their BBB Scam Tracker database and the FINRA Foundation for funding the research.

[1] The views expressed herein are her own and not necessarily those of the Commission or any individual Commissioner.

Summary

Victimization by scams and fraud depends, in part, on two-way engagement between the target of the scam and the fraudster. Some individuals simply do not engage with a scammer; others engage but at some point recognize the deception and cease engagement. Still others engage with the fraud and lose money (sometimes a lot of money). Despite the enormous personal and financial costs of fraud victimization, little is understood about the factors that differentiate these three groups.

In this survey of 1,408 Americans and Canadians who were targeted and reported a scam, nearly half (47 percent) did not engage with the fraudster and so were not victimized. Thirty percent engaged but did not lose money, yet 23 percent engaged and ultimately lost money. The type of scam and the method by which the respondents were exposed to the offer were highly associated with engaging and losing money. Specifically, scams involving online purchases correlated with the highest levels of engagement and victimization. With regard to modality, survey respondents who engaged and became victims were more likely to report being exposed to those scams on a website or through social media than via telephone, mail, or email. Social isolation and low levels of financial literacy were also associated with engaging and losing money. This research also found that prior knowledge of scams and fraud can reduce susceptibility.

BACKGROUND

Approximately one in ten U.S. adults are victims of fraud each year (Anderson, 2013), and self-reported fraud loss complaints to the Federal Trade Commission's (FTC) Consumer Sentinel Network increased by about 34 percent from 2017 to 2018 (authors' calculations using FTC consumer complaint data). The FTC received more than 372,000 fraud complaints with more than $1.5 billion in direct losses in 2018, and another 1.1 million fraud complaints with no reported losses (FTC, 2019).

In 2017 and 2018, the FINRA Investor Education Foundation, in concert with BBB Institute for Marketplace Trust and the Stanford Center on Longevity, sponsored a study to uncover the process of fraud victimization and understand the factors associated with losing money. The study involved a comparison of those exposed to a scam who lost money (victims) to those exposed to a scam who successfully avoided losing money (targets). The goal of the research was to better understand the conditions under which scam targets do not become victims in order to develop more focused and effective public education based on those protective factors.

All participants in this two-phase study reported a fraud to BBB Scam Tracker℠, an online fraud reporting tool of the Better Business Bureau. The first phase of the research comprised one-hour interviews with 18 consumers, some of whom reported being a scam victim (monetary loss) and others who reported being targets but not victims (no monetary loss). In the second phase of the study, the research team administered a 15-minute online survey to 1,408 consumers who filed a fraud tip or report through BBB Scam Tracker (see Methodology section for more details). The survey questions were informed by the qualitative findings from the first phase of the research, and the survey results are the focus of this issue brief. The survey sample skewed older, female, and college-educated. Sample sociodemographic characteristics are shown in Appendix A.

The most common scams that participants in the survey reported to BBB Scam Tracker were tech support (n=225), bogus tax collection (i.e., "the IRS scam"; n=200), phishing (n=200), and online purchase scams (n=158).[2]

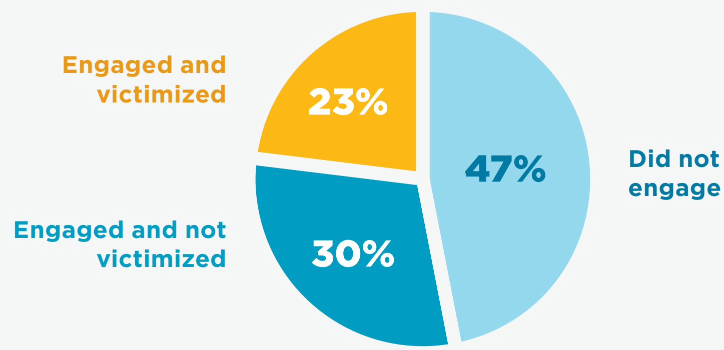
[2] Prevalence and victimization rates reported in this brief refer only to the survey sample. They do not reflect the rates of victimization for all individuals who reported fraud to BBB Scam Tracker. This information can be found in the annual BBB Scam Tracker Risk Reports available at **BBB.org/BBBScamTrackerRiskReport**.

FACTORS RELATED TO VICTIMIZATION

Level of Engagement

The first step to being victimized by a scam is to engage with a fraudster, so it is heartening to see that nearly half (47 percent) of survey respondents rejected the offer outright (Figure 1). They hung up the phone, closed the link, ignored the email, threw away the mailer, deleted the friend request, or otherwise refused to comply. This refusal to engage was the predominant response in bogus tax and other debt collection scams, and in phishing scams where fraudsters impersonate a trustworthy entity to mislead the target into giving them money. However, 30 percent of respondents engaged to some degree, but ultimately did not lose money, while 23 percent engaged with the fraudster or offer and lost money.

FIGURE 1
Engagement in the Fraudulent Offer



NOTE: 33 respondents could not be categorized due to their uncertainty about the incident.

It is heartening to see that **nearly half** of survey respondents rejected the scam offer outright.

Type of Scam

Victimization rates in this sample varied dramatically by scam type. Among the fraud categories with more than 50 respondents, the highest victimization rates were online purchase scams, tech support scams, employment scams, and fake check/money order scams (Table 1).[3] The victimization rates were very low for phishing and tax collection scams.

Median losses in this survey were $600, while median losses in the *2018 BBB Scam Tracker Risk Report* were only $152. Those who filed BBB Scam Tracker reports with higher loss amounts may have been more motivated to respond to the survey to share their experience.

The highest victimization rate was online purchase scams.

TABLE 1

Engagement and Victimization Rates by Scam Type

SCAM TYPE	% ENGAGED	% LOST MONEY	# OF REPORTS
Online Purchase	84%	47%	157
Tech Support	64%	32%	225
Employment	81%	25%	106
Fake Check / Money Order	64%	22%	106
Sweepstakes / Lottery / Prizes	59%	15%	54
Debt Collection	38%	12%	112
Phishing	18%	4%	199
Tax Collection	15%	3%	200

[3] See Appendices B and C for counts of all the scam types reported and descriptions of the scam types.

Method of Contact

Whether or not a person engaged with the scam and lost money was highly associated with the method in which they were exposed to the offer (Table 2). Phone and email were the most common methods of contact, but relatively few respondents reported losing money as a result of these scams. For example, 39 percent of respondents who said they were contacted by phone engaged with a scammer and only 11 percent lost money. In contrast, of those contacted by email, 42 percent engaged with the scammer and only 13 percent lost money. Of those who said they were exposed to a scam on social media, 91 percent engaged and 53 percent lost money. Similarly, 81 percent of respondents who were exposed to a fraud via a website said they engaged and 50 percent lost money.

81% of respondents who were exposed to a fraud via a website said they engaged.

TABLE 2

Engagement and Victimization Rates by Type of Contact

HOW THE SCAM BEGAN	% ENGAGED	% LOST MONEY	# OF REPORTS
Phone Call / Voice Mail	39%	11%	553
Email	42%	13%	340
Website	81%	50%	123
Social Media	91%	53%	70
Postal Mail	40%	12%	58

NOTE: We did not compute statistics for categories with less than 50 observations. Number of reports does not total 1,408 due to missing data on how the scam began.

Self-Reported Reasons for Engaging

Using a seven-point Likert scale, where "1" was strongly disagree and "7" was strongly agree, we asked those who engaged with the scam a series of questions to understand the factors leading to monetary loss.

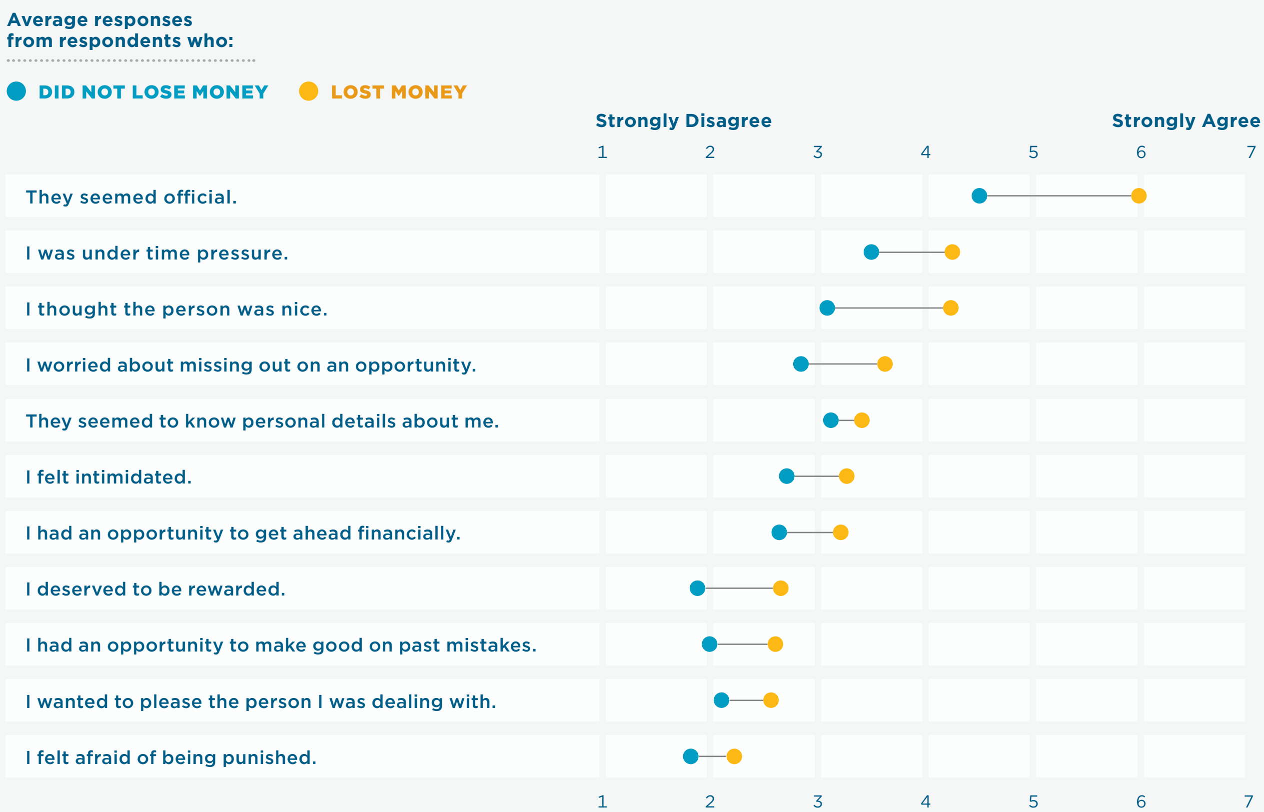
As shown in Figure 2, on a range of factors that the qualitative portion of this study suggested were related to fraud victimization, respondents who engaged and lost money scored higher than respondents who engaged and did not lose money. For example, the more a respondent felt that the person/organization seemed official, the more likely they were to lose money. Respondents were also more likely to lose money the more they felt under time pressure, believed the opportunity would help them get ahead financially, felt that it was "their time" and that they deserved to be rewarded, wanted to make good on past mistakes, and/or were intimidated by the person they were dealing with. Those who lost money were also more likely to agree that they wanted to impress the person they were dealing with and worried about missing out on an opportunity. All of these differences were statistically significant at $p<.01$. These findings align with common persuasion techniques that fraudsters use to convince targets to comply (Cialdini, 2001).

> *"Sounded like a sheriff's deputy and he was threatening me with immediate arrest if I didn't comply."*

> *"I was caught off guard and insufficiently informed."*

FIGURE 2

Perceptions of the Fraudster and the Scam Associated with Financial Loss



Demographics

We found small to no difference in engagement behavior or victimization rates by gender, ethnicity, education, or employment status, though we did find an age-based effect. On average, those who lost money were 2-3 years younger than those who were targeted for a scam but did not engage.[4] This is consistent with published data on fraud reports to both the FTC's Consumer Sentinel Network and BBB Scam Tracker — older adults report more scams in which they were targeted but not victimized compared to younger adults who are more likely to report scams that resulted in financial loss (BBB Institute, 2019; FTC, 2019). Further, those who engaged and lost money were less likely to be married and more likely to be widowed or divorced.

Respondents were more likely to be victimized **if they did not have anyone to discuss the offer with.**

Respondents were more likely to be victimized if they did not have anyone to discuss the offer with. It is noteworthy that single, divorced, and widowed respondents were more likely to indicate that they did not have anyone to discuss things with compared to married respondents and those living with a partner. Those who engaged, in general, and those who lost money expressed significantly higher feelings of loneliness. Specifically, losing money was associated with more frequent feelings of being left out, lacking companionship, and being isolated from others (meanvictim=4.5, meannon-victim=4.0 , p<.001).[5]

Financial Insecurity

Prior work by Anderson (2013) and AARP (2003) has indicated that individuals who are under financial strain might be more susceptible to scams, especially scams that promise financial rewards or an opportunity to get out of debt. In the present study, low household income ($50,000 and below) was significantly associated with engaging and losing money in a scam (p<.001). In addition, those who lost money were significantly more likely than non-victims to show signs of financial insecurity. This included reporting that they spend more than their monthly income (23 percent versus 17 percent; p=.017), and that they "probably could not" or "certainly could not" come up with $2,000 if an unexpected need arose within the next month (38 percent versus 20 percent; p<.001).

Victims were also significantly more likely to agree with the statement "I have too much debt right now" ($mean_{victim}$=3.6 $mean_{non\text{-}victim}$=3.1 out of seven, p=.001). Levels of financial insecurity varied by scam type. For example, respondents who reported advance fee loan, investment, and sweepstakes/lottery/prizes scams were more likely than other reporters to show signs of financial insecurity. It is also possible that the scams themselves contributed to the financial insecurity of the victims.

"I was overwhelmed with student loan debt."

[4] Compared to the average individual who reported fraud to BBB Scam Tracker, the survey sample skewed older. Age differences would likely be greater if the sample was representative of all reporters in the BBB Scam Tracker database.

[5] Respondent scores on these three loneliness items (range=1-3) were summed for the analysis (range=3-9).

Financial Literacy

Participants were asked five questions to gauge their financial knowledge. As seen in Figure 3, those who ended the scam attempt immediately scored significantly higher on this five-item quiz, an average of 3.3 correct answers out of a total of five.[6] The average score of those who engaged with the scam was 3.0, and of those who lost money was 2.7 ($p<.001$).[7]

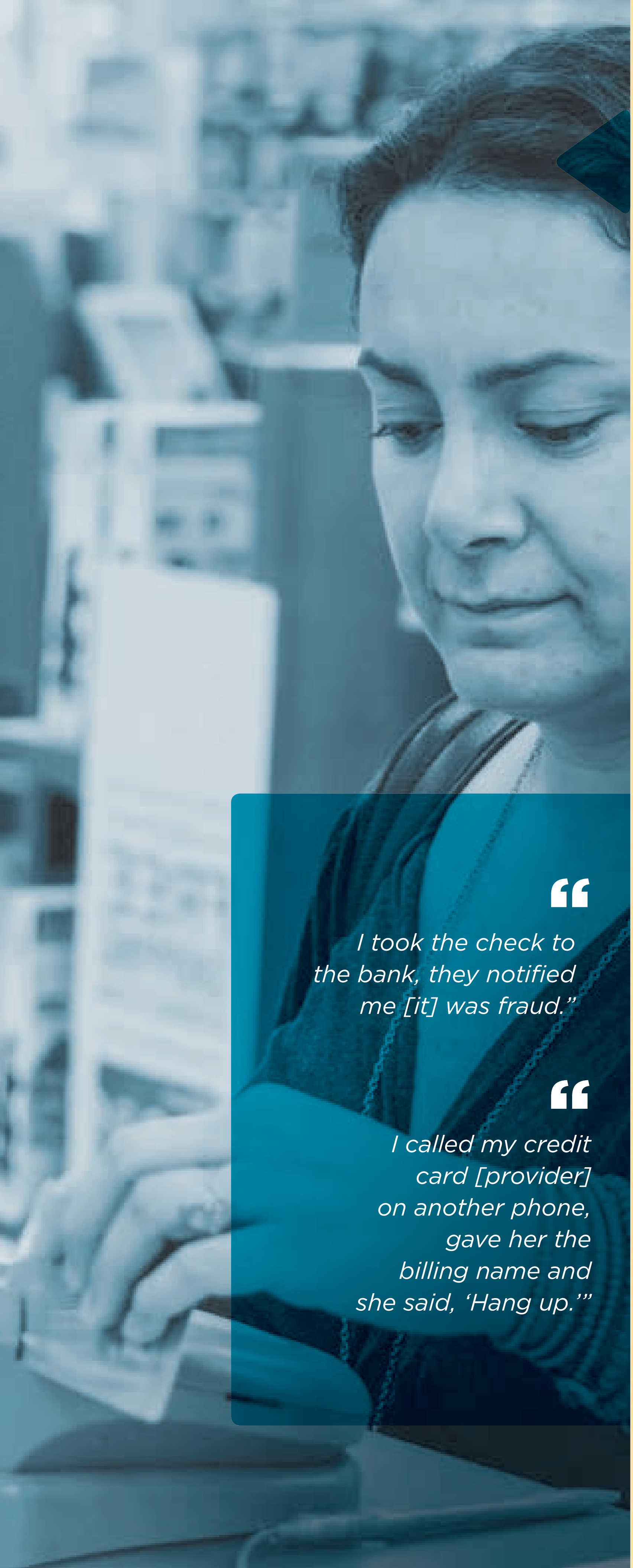
FIGURE 3

Financial Literacy by Engagement: Mean Number of Questions Answered Correctly Out of 5

Those who ended the scam attempt immediately **scored significantly higher.**

[6] The five financial literacy quiz questions can be found at **USFinancialCapability.org/quiz.php**.

[7] Kieffer and Mottola (2017) and AARP (2007) found that higher levels of financial literacy were associated with higher fraud victimization rates. However, these papers examined investment fraud, and it is possible that some victim characteristics vary by scam type. Investment fraud victims make up less than 2 percent of the current sample.



Intervention By Organizations — The Role Of Structural Protections

Among those who engaged with the scam, 20 percent reported that an organization, company, or agency intervened or tried to intervene to stop the scam. People described interventions by bank tellers and employees of wire transfer services and other financial services companies. Some organizations train their frontline employees to recognize the indicators of fraud (e.g., large cash bank withdrawals or purchases of high-dollar value gift cards). The survey results show that 51 percent of people who reported a third-party intervention were able to avoid losing money. This is a promising finding given that these interventions generally occur at a point when consumers are on the cusp of sending money to a scammer (e.g., at a store checkout counter buying gift cards). The work of cashiers, bank tellers, and other vigilant employees can serve as an important last line of defense for consumers who might otherwise become fraud victims.

We know from previous studies that individuals engaging with scammers are likely to be in a heightened emotional state that impairs their ability to respond appropriately to misleading information (Kircanski et al., 2018). Further, in many cases, fraudsters have developed scripts designed to negate intervention by third parties, such as telling their targets not to speak to anyone and even coaching them on how to respond to a cashier's or bank teller's questions and protests. Additional research in this area could help businesses and others who are well-positioned to intervene to develop more effective training programs and intervention techniques.

PERCEPTION OF VICTIMS

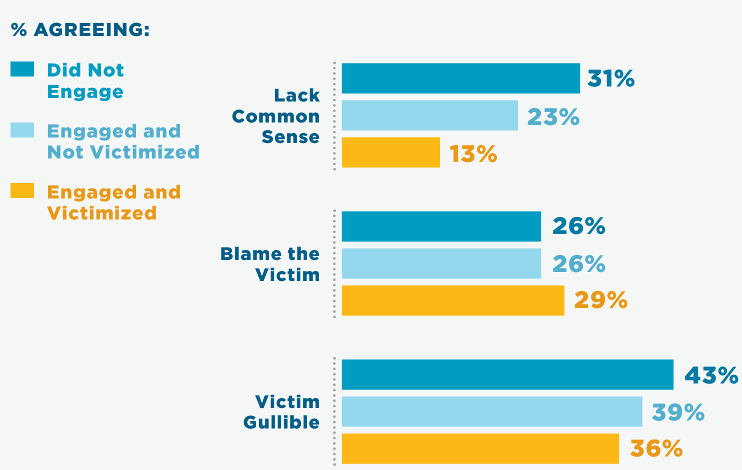
> *"Looking back, it was so obvious that it was a scam. I guess I wanted it to be true. I didn't read the comments until it was too late. I'm so embarrassed."*

The survey also sought to gauge how respondents view scam victims, in general. A large percentage of respondents believe that victims of fraud are gullible — from a high of 43 percent for those who did not engage to a low of 36 percent for those who lost money (Figure 4). It is noteworthy that nearly a third of those who lost money believe it is likely the victims' fault for being defrauded. When asked if scam victims lack common sense, only 13 percent of victims believe that to be true, compared to a third of those who did not engage.

Reporting rates for fraud and scams are low, and it is possible that widely held negative views associated with victims contributes to a person's reluctance to admit that they were scammed. This could also deter victims from seeking assistance in dealing with the consequences of fraud, whether financial, psychological, or emotional assistance. Earlier work by the FINRA Foundation (2015) found that the non-financial costs of fraud (e.g., stress, health problems) are widespread among victims, and nearly two-thirds (65 percent) report experiencing at least one type of non-financial cost to a serious degree. The FINRA Foundation study also found that 47 percent of victims blamed themselves. These findings suggest that victim support groups could play an important role in destigmatizing the experience and helping those who have lost money recover from fraud.

FIGURE 4

How Victims Are Viewed



PREVENTING FINANCIAL FRAUD

Knowledge is Power

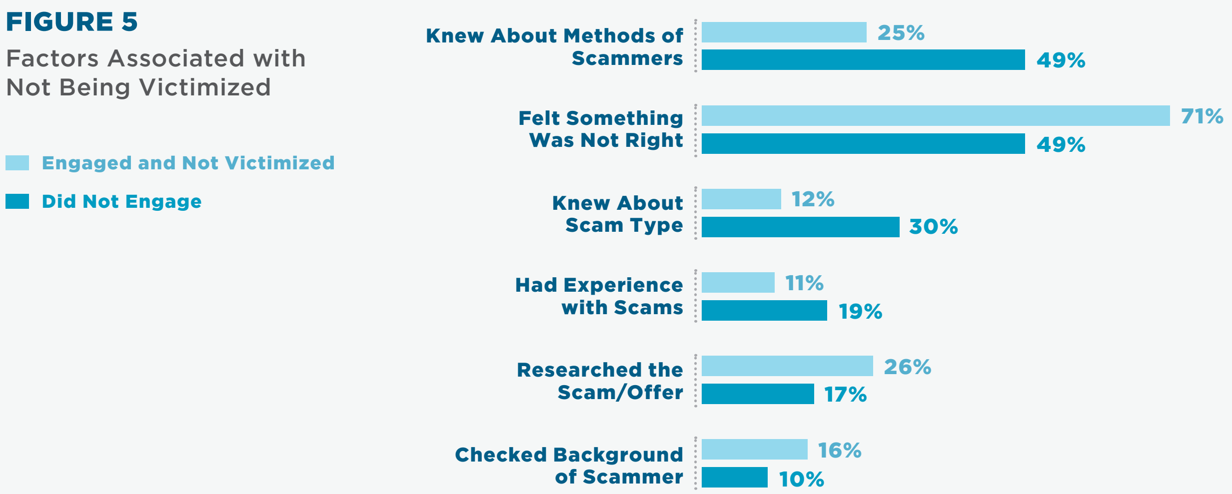
Knowing about specific types of scams and understanding the general tactics that scammers use can help a scam target avoid becoming a victim. In this survey, 30 percent of respondents who did not engage knew about the scam before they were targeted compared to 12 percent of people who engaged but were not victimized (Figure 5). Respondents who had heard about the scam before were significantly less likely to lose money (9 percent versus 34 percent, $p<.001$). Among respondents who did not engage with the scammer, almost half (49 percent) reported knowing about the methods and behaviors of scammers in general compared to only 25 percent of those who did engage but were not victimized. Those who did not engage were also more likely to say they had experience with scams than those who engaged but were not victimized, 19 percent versus 11 percent, respectively. This indicates that having prior knowledge about fraud, even generally, is particularly helpful in avoiding victimization.

> *I suspected it was a scam very early on, but I didn't pay attention to my instincts."*

The majority of fraud targets did not report looking into the scam or the scammer while they were being targeted. For instance, among those who did not engage, 17 percent researched the offer and 10 percent checked the background of the scammer. For those who engaged but were not victimized, 26 percent researched the offer, and 16 percent checked the background of the scammer. Last, among those who engaged but were not victimized, by far the most common reason cited for not being victimized was that they felt something was not right about the situation.[8]

FIGURE 5

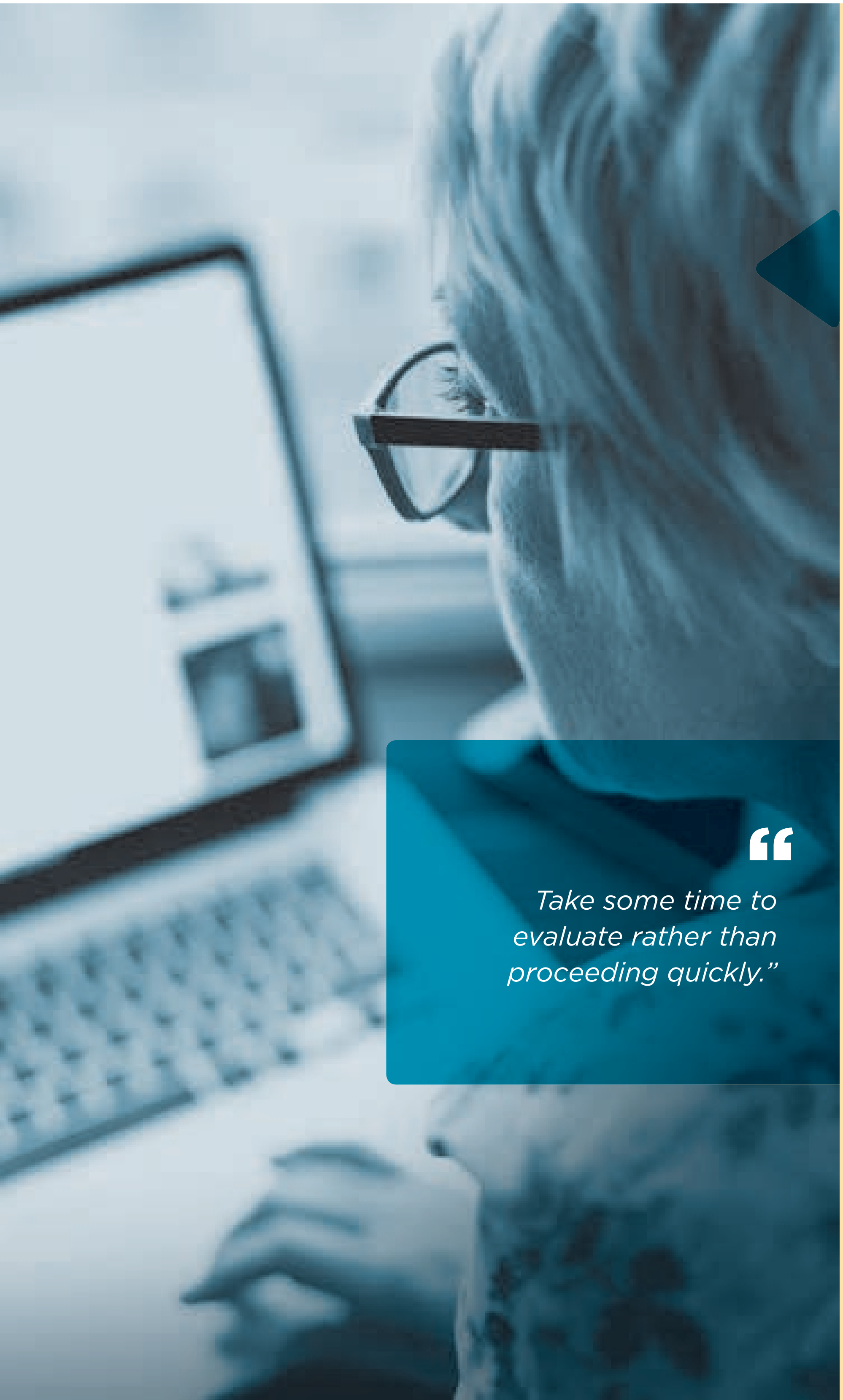
Factors Associated with Not Being Victimized



[8] We do not have these data on victims because we logically could not ask victims what helped prevent them from being victimized.

Among respondents who engaged, those who *chose not* to discuss the solicitation with anyone while it was happening were significantly more likely to lose money, as were those who *did not have anyone available* to discuss it with.

"I talked to my kids and they said they were pretty sure it was a scam."



"Take some time to evaluate rather than proceeding quickly."

In the Targets' Own Words

Respondents who were suspicious about the offer but who continued to engage were asked what would have helped them avoid engaging altogether. One individual stated, "…if I had done the research before making the purchase." Other suggestions were to speak with someone prior to engaging, use other websites to verify the pricing of the product, check the BBB website for complaints about the organization, and search for the address of the organization on Google Maps. One person said, "not being distracted." Recommendations also included looking for clues that the offer is fake, such as misspelled words in the message or a spoofed email address.

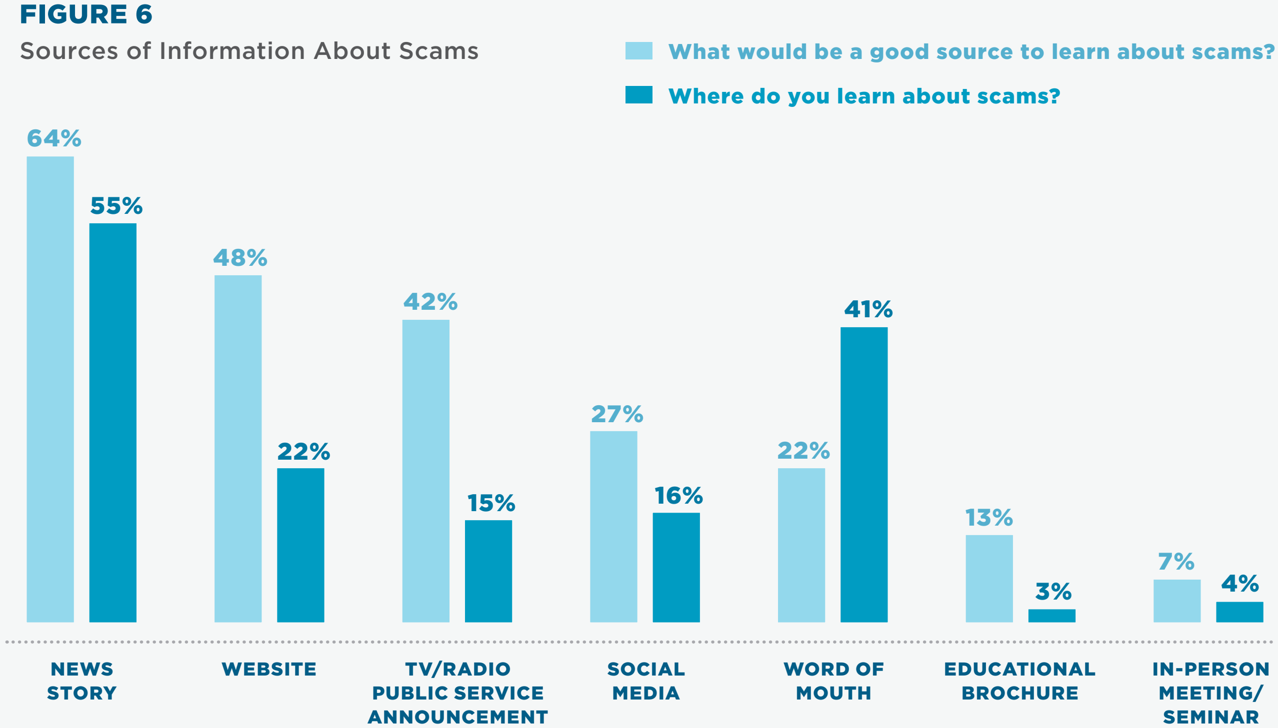
Where do victims and non-victims learn about fraud?

We asked respondents what they believed would be a good source of information on fraud and scams, and where they have actually received such information. While nearly half (48 percent) believed websites would be a good source of information, few actually reported obtaining information about fraud and scams from websites (Figure 6). It is noteworthy that 42 percent of respondents believed that a public service announcement (PSA) on TV or radio would be helpful, but few respondents (15 percent) noted this as an actual source of information where they previously learned about fraud, likely because PSAs about scams are not very common. News stories were, by far, the most popular answer. Conversely, while respondents did not believe word of mouth is a particularly good source of information about scams, more than 40 percent of respondents said they had obtained information about frauds in this way. Educational brochures and in-person meetings/seminars were infrequently mentioned as good or actual sources of information about scams and fraud. However, they may have an indirect effect on reducing fraud by fueling the communication of information on frauds by word of mouth. While it is beyond the scope of this study to determine the actual effectiveness of sources of information, these findings suggest that the news media has an important role to play in making consumers aware of scams.

News stories were, by far, the most popular answer.

FIGURE 6

Sources of Information About Scams



IMPLICATIONS

In terms of protective factors, **knowledge is power.**

The path to victimization begins with engagement, and there are a number of factors that increase the likelihood of both engaging with a fraudulent offer and losing money.

- **The manner in which consumers are contacted plays a significant role in whether or not they engage and become victims.** Because those contacted via digital means (social media and website) appear from this study to have high engagement and victimization rates, consumers should be particularly careful when sending money based on a digital message or ad.

- **The perception that a fraudster is "official" is highly associated with victimization.** As titles and designations are easily faked, consumers should independently verify the identity of anyone who claims to be an authority and asks for money or information (e.g., call the agency directly to confirm, or use an online tool such as FINRA BrokerCheck).

- **Financial insecurity** appears to increase the likelihood of victimization, as do **low levels of financial literacy.**

- **More than half of people who reported a third-party intervention were able to avoid losing money.** This is a promising finding and speaks to the potential of this approach to reduce fraud victimization given these interventions generally occur at a point when consumers are on the cusp of sending money to a scammer.

- **In terms of protective factors, knowledge is power.** Prior knowledge about fraud, even generally, is particularly helpful in avoiding victimization.

- **Before complying with a solicitation, consumers should consult with those around them** to verify the legitimacy of the offer or the threat. This strategy is helpful because it harnesses collective knowledge about scams and persuasion tactics from friends, family, neighbors, and whoever else is present at the time of the solicitation. These people might encourage the target to pause and take time to assess the situation.

Incorporating these protective behaviors into routine interactions with sellers and other agents of influence could help consumers avoid fraud, but knowing about common scams and the tactics of persuasion ahead of time is potentially even more effective at preventing fraud than doing research in the moment. “Trusting your gut” when you sense something might be wrong with a situation can also serve as a protective factor. However, if your instincts are leading you in the opposite direction and telling you to engage, “trusting your gut” could lead to victimization. Therefore, a wise strategy is to pause, talk it over with others, and do some research before sending any money or sharing personally identifiable information.

Further, given the generally negative perception of victims, support groups can help individuals who have experienced fraud cope with the social and emotional consequences. And the news media can play a role in spreading awareness of how to spot, avoid, and report scams. The media can also help send an empowering message, and perhaps change the negative stigma associated with victimization, by giving people who have experienced a scam the opportunity to help others by sharing their story.

Knowing about common scams and persuasion tactics ahead of time is **potentially even more effective** at preventing fraud than doing research in the moment.

METHODOLOGY

More than 90,000 individuals who submitted a fraud report to BBB Scam Tracker between 2015 and 2018 were invited by email to participate in a 15-minute survey seeking to understand why people are targeted for scams, with the goal to craft better interventions for safeguarding people against them. The survey was fielded in August 2018, and we received 1,408 eligible responses.[9] Before entering the survey, participants read an online consent form and agreed to participate. The study was reviewed and approved by Sterling IRB. No personally identifying information was collected. Respondents who initially submitted a fraud report to BBB Scam Tracker on behalf of someone else, meaning that they were not the targets of the solicitation, were discontinued from the survey.

While the sample size is large enough to detect statistically significant differences between groups, we caution that this does not mean that the findings are representative of the broader population of fraud targets and victims. As a result of response bias, which is common to many surveys, those who responded might differ from individuals who did not submit a fraud report to BBB Scam Tracker and those who do not recall or acknowledge losing money in a scam at all. Future studies should compare these findings with findings using samples of independently identified victims.

Prior to fielding the survey, 18 individuals recounted their experience with scam attempts during in-depth interviews (conducted in person or online via video). These first-hand accounts, video-recorded either in the subjects' homes, at locations near their homes, or online, vividly chronicled the persuasion tactics scammers used; revealed situational characteristics of the scam encounters; and surfaced the personal knowledge, beliefs, and values of the scam targets themselves, all potential factors in the outcome of scam attempts.

[9] Responses were dropped if the respondent did not complete the survey or if they did not answer a data integrity check question correctly.

AUTHORS

Marti DeLiema, Ph.D., is an assistant professor of research at the University of Minnesota, Twin Cities, in the School of Social Work. Her research focuses on identifying the correlates of financial fraud in the US and the factors related to elder financial victimization. Dr. DeLiema received her Ph.D. in gerontology from the USC Davis School of Gerontology and completed a postdoc at the Stanford Center on Longevity.

Emma Fletcher joined the Federal Trade Commission's Bureau of Consumer Protection in 2017 as a Presidential Management Fellow. She previously served in the Division of Consumer and Business Education and currently serves in the Division of Consumer Response and Operations, focusing on projects at the intersection of data analysis and consumer education. Ms. Fletcher has authored several of the FTC's *Consumer Protection Data Spotlight* publications, exploring trends seen in reports to the FTC's Consumer Sentinel Network. She previously worked as the director of scam and fraud initiatives at the Better Business Bureau. Ms. Fletcher received her B.S. in psychology from James Madison University and holds a master's degree in public administration from George Mason University.

Christine N. Kieffer is senior director of the FINRA Investor Education Foundation with 20 years of financial and investor education experience. She manages national, state, and grassroots partnerships, and develops tools and programs for law enforcement, victim advocates, and consumers to advance investor protection and fraud prevention initiatives. Her role includes directing research, primarily related to financial fraud. Ms. Kieffer also oversees financial readiness programs for military families and other underserved audiences. Ms. Kieffer received her B.S. from Vanderbilt University with double majors in economics and mathematics.

Gary R. Mottola, Ph.D., is the research director for the FINRA Investor Education Foundation and a social psychologist with more than 25 years of research experience. In his role at the FINRA Foundation, he oversees and conducts research projects aimed at better understanding financial capability in America, protecting investors from financial fraud, and improving financial disclosure statements. Dr. Mottola received his B.A. from the University at Albany, M.A. from Brooklyn College, and Ph.D. from the University of Delaware. He was a visiting scholar at Wharton in 2006 and is an adjunct professor of statistics in Villanova University's MBA program.

Rubens Pessanha, Ed.D., MBA, PMP, GPHR, SPHR, SHRM-SCP, senior director of research & development at the International Association of Better Business Bureaus, has more than 20 years of global experience in marketing, strategic organizational development, project management, and market research. He has presented at conferences in North America, Asia, Europe, Africa, and South America. A production engineer with an MBA, he completed his doctorate at George Washington University. He is the co-author of the *BBB Scam Tracker Risk Report* (2016 and 2017), *Scams and Your Small Business* (2018), *Cracking the Invulnerability Illusion* (2016), *The State of Cybersecurity* (2017 and 2018), the BBB Trust Sentiment Index (2017), *5 Gestures of Trust* (2018) and the BBB Industry Research Series - Airlines (2018). As a hobby, Dr. Pessanha teaches project management, business ethics, strategy and marketing for graduate and undergraduate students.

Melissa "Mel" Trumpower is executive director of the BBB Institute for Marketplace Trust, the educational foundation of the Better Business Bureau. In addition to overseeing BBB Institute, Ms. Trumpower manages the BBB Scam Tracker program and is co-author of the *BBB Scam Tracker Risk Report* (2017 and 2018) and *Scams and Your Small Business* (2018). Ms. Trumpower has more than 25 years of nonprofit leadership experience, working with a wide range of nonprofit organizations and trade associations, including Good360, the National Wildlife Federation, IFES, and the National Endowment for Democracy. Ms. Trumpower has a B.S. from Cornell University and a M.A. from Johns Hopkins University.

REFERENCES

AARP (2003). *Off the Hook: Reducing Participation in Telemarketing Fraud*. AARP Consumer Education: Washington, DC. Retrieved from **https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf**

AARP (2007). *Stolen Futures: An AARP Washington Survey of Investors and Victims of Investment Fraud*. Washington, DC: AARP.

Anderson, K. B. (2013). *Consumer Fraud in the United States, 2011: The Third FTC Survey*. Federal Trade Commission, Washington, DC. Retrieved from **https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf**

BBB Institute for Marketplace Trust (BBB Institute) (2019). *Tech-Savvy Scammers Work to Con More Victims: Scam Tracker Risk Report* (2018). **https://www.bbb.org/bbbscamtrackerriskreport**

Cialdini, R. B. (2001). *Influence: Science and Practice* (4th ed.). Boston: Allyn and Bacon.

Federal Trade Commission (FTC) (2019). Consumer Sentinel Network data visualizations as of March 31, 2019. Washington, DC. Retrieved from **https://public.tableau.com/profile/federal.trade.commission#!/**

FINRA Investor Education Foundation (2015). *Non-Traditional Costs of Financial Fraud: A Report of Survey Findings*. Applied Research and Consulting. Retrieved from **https://www.saveandinvest.org/file/document/non-traditional-costs-financial-fraud-survey-findings**

Kieffer, C. and Mottola, G. (2017). Understanding and Combating Investment Fraud. In O. Mitchell, P. Hammond, and S. Utkus (eds.), Financial Decision Making and Retirement Security in an Aging World. Oxford: Oxford University Press, pp. 185-212.

Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola, G., and Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and Aging*, 33(2), 325–337.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, 80(1), 1–28.

APPENDIX A

Sample Characteristics

SOCIODEMOGRAPHIC CHARACTERISTIC	STATISTIC
Average Age	56
Female	66%
Household Income > $50,000	55%
College Degree	73%
Non-Hispanic White	80%
Married	54%
Unemployed	3%

APPENDIX B

Scam Types Reported

SCAM TYPE	NUMBER OF REPORTS
Tech Support	225
Tax Collection	200
Phishing	199
Online Purchase	157
Other[10]	127
Debt Collection	112
Employment	106
Fake Check/Money Order	106
Sweepstakes/Lottery/Prizes	54
Government Grant	36
Advance Fee Loan	32
Travel/Vacations	31
Investment	23

[10] Respondents were asked to select the type of scam they reported to BBB Scam Tracker. In order to reduce the cognitive burden of completing the survey, scam categories that were not well-represented in BBB Scam Tracker were not presented to the respondents. As a result, fewer than half of BBB Scam Tracker's scam categories were presented to respondents. If the respondent did not see their scam, they had the option of choosing "Other" and specifying the scam in writing. As expected, the "Other" category made up less than 10 percent of the total responses. For a list and description of all scams reported to BBB Scam Tracker, see *Tech-Savvy Scammers Work to Con More Victims: BBB Scam Tracker Risk Report* (2018).

APPENDIX C

Scam Type Descriptions

ADVANCE FEE LOAN	In this scam, a loan is guaranteed but once the victim pays upfront charges such as taxes or a "processing fee," the loan never materializes.
DEBT COLLECTION	In this scam, phony debt collectors harass their targets, trying to get them to pay debts they don't owe.
EMPLOYMENT	Targets are led to believe they are applying or have just been hired for a promising new job while they have, in fact, given personal information or money to scammers for "training" or "equipment." In another variation, the target may be "overpaid" with a fake check and asked to pay back the difference.
FAKE CHECK/ MONEY ORDER	In this scam, the victim deposits a phony check and then returns a portion by wire transfer to the scammer. The stories vary, but the victim is often told they are refunding an "accidental" overpayment. Scammers count on the fact that banks make funds available within days of a deposit, but can take weeks to detect a fake check.
GOVERNMENT GRANT	In this scam, individuals are enticed by promises of free, guaranteed government grants. The only catch is a "processing fee." Other fees follow, but the promised grant never materializes.
INVESTMENT	These scams take many forms, but all prey on the desire to make money without much risk or initial funding. "Investors" are lured with false information and promises of large returns with little or no risk.
ONLINE PURCHASE	These scams involve purchases and sales, often on eBay, Craigslist, Kijiji or other direct seller-to-buyer sites. Scammers may pretend to purchase an item only to send a bogus check and ask for a refund of the "accidental" overpayment. In other cases, the scammer will simply never deliver the goods.
PHISHING	Scammers send communications that impersonate a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information or passwords.
SWEEPSTAKES/ LOTTERY/PRIZES	This scam fools victims into thinking they have won a prize or lottery jackpot, but need to pay upfront fees to receive the winnings, which never materialize. Sometimes this con involves a fake check and a request to return a portion of the funds to cover fees.
TAX COLLECTION	In this scam, imposters pose as government tax collection agents and use threats of immediate arrest or other scare tactics to convince their targets to pay, often requesting that the target load money onto gift cards as payment.
TECH SUPPORT	Tech support scams start with a call or pop-up warning that alerts the target to a computer bug or other problem. Scammers pose as tech support employees of well-known computer companies and hassle victims into paying for "support." If the victim allows remote access, malware may be installed.
TRAVEL/ VACATIONS	Scammers post listings for properties that either are not for rent, do not exist, or are significantly different than pictured. In another variation, scammers claim to specialize in timeshare resales and promise they have buyers ready to purchase.

ABOUT THE STANFORD CENTER ON LONGEVITY

Longer lives are, at once, among the most remarkable achievements in all of human history, and the greatest challenges of the 21st century. Whereas most discussions about aging societies are premised on the assumption that older people are frail and infirm, our premise is that problems of older people demand solutions so that the substantial increase in life expectancy can ultimately benefit individuals and societies. The mission of the Stanford Center on Longevity is to accelerate and implement scientific discoveries, technological advances, behavioral practices, and social norms so that century long lives are healthy and rewarding.

Longevity.Stanford.edu

ABOUT THE FINRA INVESTOR EDUCATION FOUNDATION

Established in 2003 by the Financial Industry Regulatory Authority, the FINRA Investor Education Foundation empowers underserved Americans with the knowledge, skills and tools to make sound financial decisions throughout life. The Foundation accomplishes this mission through educational programs and research that help consumers achieve their financial goals and that protect them in a complex and dynamic world.

FINRAFoundation.org

ABOUT THE BBB INSTITUTE FOR MARKETPLACE TRUST

The BBB Institute for Marketplace Trust (BBB Institute) is the educational foundation of the Better Business Bureau. BBB Institute works with local, independent BBBs across North America to deliver educational programs that foster a trusted marketplace by empowering consumers to take control of their purchasing decisions and avoid scams, helping businesses deliver excellent service with integrity and become integral stakeholders in their communities, and publishing research that provides critical insights for the average consumer.

BBBMarketplaceTrust.org

FINRA Investor Education FOUNDATION

BBB INSTITUTE for MARKETPLACE TRUST

STANFORD CENTER ON LONGEVITY