Recognizing the Stressful Life Events, Emotions and Actions that Make Us Susceptible to Scams: An AARP National Fraud Frontiers Report

DOI: HTTPS://DOI.ORG/10.26419/RES.00484.001
An AARP National Fraud Frontiers Report

A MOMENT’S NOTICE
Recognizing the Stressful Life Events, Emotions and Actions that Make Us Susceptible to Scams

TABLE OF CONTENTS
4 Executive Summary
6 Introduction
12 Part One: How Much Fraud is Out There?
18 Part Two: What Makes Us Susceptible to Fraud?
30 Part Three: Which Protective Factors Might Impact Our Susceptibility to Fraud?
36 Part Four: Which Risk Factors Best Predict Fraud Susceptibility?
40 Implications, Methodology, Appendix

AUTHORS
Report written by Doug Shadel, PhD, Alicia Williams, PhD, Karla Pak, PhD, and Lona Choi-Allum, PhD

ACKNOWLEDGMENTS
Special thanks to Alison Bryant, SVP AARP Research, for giving us the opportunity to take a more in-depth look into what makes consumers more susceptible to fraud. Sincere appreciation to Jeff Love, Director of Financial Resilience, AARP Research, for his invaluable leadership and guidance in getting this study off the ground. Thanks to Indira Venkat, VP of Consumer Insights, for her keen insights throughout the study process. We are especially grateful to Kathy Stokes, Amy Nofziger, and Mark Petterhoff, who offered their expertise and insights on the survey questions and final report. Many thanks to Chuck Rainville for the countless hours he spent assisting us in analyzing the data, Sibora Gjecovi for providing population estimates across various demographic categories, and Brian Meekins for creating population weights for our incidence findings. Thanks to Laura Carstensen from the Stanford Center on Longevity for her early input into the survey design. Sincere thanks to Kristy Holtfreter and Mike Reisig from Arizona State University, who provided feedback to our survey instrument. Thanks to Neil Wertheimer and Jason Erskine for their invaluable advice about the report’s narrative shape and direction. Thanks to our AARP colleagues, Navendu Shekhar, Jen Sauer, Oscar Anderson, Manju Majhi, Emily James, and Gena Wright, for their collaboration and commitment which played a vital role on the final report. And thanks to the AARP Translation Services team who translated the survey instrument into Spanish, Tenesha Hill for data checking our findings, and NORC at the University of Chicago for fielding the survey.

FACTORS THAT BEST PREDICT LIKELIHOOD OF FINANCIAL LOSS TO SCAMS

Technology and business sophistication have moved scam operations from the hands of small-time crooks into a booming, multibillion-dollar transnational industry. The growth in the industry underlies the growth in fraud reports, which have skyrocketed since the wake of the global pandemic in 2020.

AARP partnered with NORC from the University of Chicago to determine how many U.S. adults lose money to scams each year, and whether there are particular risk factors that may increase fraud susceptibility. The survey reached over 9,000 Americans ages 18+, including 1,085 fraud victims*, making it one of the largest studies AARP has done on the subject of consumer fraud.

The study found that an estimated nine in ten Americans (229 million people) encountered a fraud attempt and that one in seven (33 million people) lost money to a scam in 2020 alone. Although anyone can experience a scam—regardless of education, age, race or ethnicity—the study uncovered specific environmental and emotional factors that were common among fraud victims. These include:

1. **STRESSFUL LIFE EVENTS**
   Fraud victims experienced twice as many stressful life events such as death of a family member, loss of a job, or feeling lonely during the time they encountered fraud than non-victims.

2. **LESS SOCIAL/FAMILY SUPPORT**
   Fraud victims reported significantly less family support and closeness than non-victims.

3. **STRONGER EMOTIONS**
   Victims reported far stronger emotional responses during fraud encounters than non-victims. These emotions were both positive and negative and led to more victims feeling out of control.

4. **TARGETED BY SCAMMERS**
   On average, fraud victims reported 60% more fraud encounters than non-victims.

Together, these dominant risk factors create what researchers call “vulnerable moments” in which targets are more susceptible to criminal tactics that focus on a person’s emotional triggers, recent challenges, and sense of isolation to achieve their theft. The implications of these learnings are many, including suggesting new approaches to informing the public about ways to prevent fraud.

*NOTE: Throughout this report, the term “victims” refers to persons who experienced a financial loss (i.e., spent money) as a result of a scam encounter.
FRAUD CAN HAPPEN TO ANYONE

Consumer fraud has long been a problem in the United States, with millions of Americans targeted by swindlers trying to steal their hard-earned money. In recent years, several forces have converged to make scamming easier for a new generation of swindlers. The widespread use of inexpensive robocalling and email has allowed scammers to cast a broad net and reach millions of potential victims. Massive data breaches have exposed our personal information on an unprecedented scale, allowing identity fraud to flourish and scammers to customize their pitches to match our personal wants and needs.

At the same time, technology has made it easier than ever for impostors to manipulate caller ID and email and pretend to be everything from the IRS to Amazon to the Social Security Administration. These factors have combined with a global health pandemic to create a perfect storm for fraud (fueling urgent needs, fear, uncertainty, economic stress, etc.) — and opening the door to increased fraud, scams, and security breaches. The Federal Trade Commission reports there has been a staggering 45% spike in the number of fraud reports flooding into their Consumer Sentinel Network in 2020 alone (see chart 1).  

CHART 1: CONSUMER SENTINEL FRAUD REPORTS (UNITS IN MILLIONS)

2017 2018 2019 2020
2.94 3.12 3.24 4.72

Source: Federal Trade Commission

We have to stop blaming the victim through negative stereotypes. The truth is anyone can lose money to fraud given the right scammer and the right moment in time.
— KATHY STOKES, DIRECTOR, AARP FRAUD PREVENTION PROGRAMS

While local, state, and federal law enforcement agencies continue to pursue scammers, many prosecutors describe these efforts as playing a game of whack-a-mole: just when they take down one fraudulent boiler room, five more pop up somewhere else around the world to take their place.  

Given that prosecution alone will not solve the fraud problem, numerous government agencies and advocacy groups like AARP have developed consumer education content designed to help people spot and resist such malicious attacks. AARP has done extensive interviews in the past with
the scammers themselves and analyzed thousands of tape recordings of the sophisticated persuasion tactics they use. This research has shown that while the scams change constantly to fit what is going on in the news, a stable set of tactics are consistently employed in most scams such as the promise of wealth, the need to act quickly, the use of pseudo-authority (impostors) and, increasingly in our anxiety-filled world, fear and intimidation.4

For the past decade, many organizations have used this research and other insights to employ a “forewarned is forearmed” strategy: the idea that if you can see a deceptive attempt coming from a distance, you are better able to defend against it. This strategy has proven effective in multiple studies. A study by AARP Foundation and the U.S. Department of Justice tested the forewarned is forearmed hypothesis by delivering fraud prevention messages to a group of consumers and comparing them to a control group that did not receive such messages. Both groups were called several days later and exposed to a fraudulent offer. The group that received the prevention message was significantly less likely to respond affirmatively to a fraud offer compared to the control group.3

A study by Stanford University looked at peer counseling provided by AARP’s Fraud Watch Network Helpline to a group of older persons who previously had lost money and then tested their resistance to a subsequent fraud attempt a month later compared to a control group. The study found a significant decrease in responsiveness by the group that had been forewarned. More recent studies by the Better Business Bureau, Stanford, and the FINRA Foundation have found similar positive impacts of the “forewarned is forearmed” approach.7

While consumer education can reduce the risk of financial loss, there are many consumers who never receive such warnings. And with fraud reports soaring in the wake of the Covid-19 crisis, there is an urgent need to better understand when and why consumers are at risk so that agencies can target messages to those who need it the most. Such insights can also help debunk some of the myths about those who experience a financial loss from fraud. Even though no single personality trait has been discovered that explains all fraud victimization, faulty generalizations abound. For example: “all scam victims are old and senile”; “all scam victims are either greedy or stupid...or both.” Such labels are not only offensive and demeaning to those who have lost money to this crime, but they are simply untrue and belie previous research that has repudiated such simplistic explanations. For example, studies conducted by AARP and the FINRA Foundation have found that while some victims are less educated and lower income, others like investment fraud victims are more likely to be highly educated, have higher incomes, and are more financially literate than the general public.7 Other studies by AARP and Microsoft have shown that while some cyber fraud victims are older, more of them tend to be younger consumers in their 30s and 40s.10

The truth is that fraud can happen to anyone and no one personality characteristic will ever likely explain all victimization. However, there may be certain risk factors that make us more susceptible to fraud. For example, studies have pointed to a correlation between fraud susceptibility and coping with stressful life events that can happen to anyone, such as divorce, illness, or loss of a job.7 The theory underlying this correlation is that coping with a stressful life event consumes valuable cognitive capacity that might otherwise be employed to spot and resist fraud.

Cybercrime researchers have found that there are particular times during the day (3–5 pm) and days of the week (Fridays) when employees are tired, their willpower is depleted, and their defenses are down. This is when scammers, posing as vendors or the HR department, are most successful at executing phishing scams.12

While it is a myth that all scam victims are older, age is a risk factor in certain types of scams like lottery, sweepstakes and health-related frauds.11 Illnesses like dementia and Alzheimer’s disease can impair decision-making, and there have been some recent neuroscience studies that show that as we age, certain parts of the brain that might otherwise spot a distrustful face or a questionable offer are less active in older people than in younger people.14 Researchers at the Stanford Center on Longevity have explored the notion that as we age, we tend to focus on more positive events and pay less attention to negative events, which is generally a useful psychological adaptation. But this dynamic can have an adverse effect when consumers weigh the risks of a particular buying decision.15

Despite these risk factors associated with aging, many millions of older people live their entire lives scam-free and surveys show
younger people have a higher victimization rate when it comes to all types of fraud.  

Another risk factor that may increase fraud susceptibility is one’s ability to manage emotions during a fraud encounter. Much of the fraud research to date has focused on cognitive factors: the ability to use one’s intellect to spot something that sounds too good to be true or assessing risk by measuring the financial literacy of victims compared to non-victims. But interviews with convicted scammers reveal that the scammer’s strategy has little to do with cognition. In fact, their goal is to get their target as far away from their cerebral cortex during a fraud transaction. Scammers want to place the target of the fraud “under the ether,” a slang term for a heightened emotional state.

Ether is a condition that a master con puts the victim under to get them to comply…it can last for three hours or three years.

— “ROCKY”, A PHONE FRAUD TRAINER IN LOS ANGELES. (SHADEL, 2012)

Veteran scammers know if the target of the fraud is in a heightened emotional state like fear or excitement, they are much easier to manipulate because they are less likely to be thinking rationally, but instead reacting emotionally. During such moments, it may not matter how much education or financial literacy one has, because the cognitive part of our brain has been sidelined and our emotions are being manipulated by skilled con artists. Only a handful of studies have pursued the “ether” theory of fraud susceptibility, but preliminary results suggest it may be an important risk factor.

Research has shown many of the conditions which increase susceptibility to fraud are the result of either unavoidable life events that may put us into a compromised position or interactions with skilled scam artists who are manipulating our emotions. But there are also certain actions that have been shown to increase fraud susceptibility. For example, separate research by AARP, the Federal Trade Commission, and criminologists from Arizona State University have found fraud victims have been more inclined to answer calls from unknown telemarketers, enter free prize contests by handing over personal information, or making remote purchases of products in response to computer pop-ups or television ads from previously unknown sellers.

The AARP Fraud Frontiers Study’s goal was to take a comprehensive look at all of the factors that may come into play in making individuals susceptible to fraud so that educators and prosecutors can develop better educational content to reduce the incidence of this crime. In October and November 2020, AARP worked with NORC from the University of Chicago and their AmeriSpeak® panel of individuals to survey over 9,000 Americans to determine how many people encounter and lose money to fraud. In the process of surveying this large sample, 1,085 scam victims and another 2,195 individuals who encountered scams but resisted were identified. This provided one of the largest samples of fraud victims AARP has surveyed in over 20 years of doing this type of research. This report summarizes the findings of this study based on four key research questions.
The AARP Fraud Frontiers Study sought to measure the percentage of the public that loses money to scams each year. Respondents were asked if they had encountered any one of 26 scenarios that a panel of fraud experts determined were scams. The scenarios were intentionally not labeled as “scams” to avoid false negatives associated with people who may not be willing to admit they lost money to a scam. Rather, respondents were simply provided a description of a scenario one might encounter in the marketplace.

For example, the IRS impostor scam was described as follows: “Someone contacted you saying that they work for the IRS and that you owe the IRS money.” Such a contact is a scam because the IRS does not call taxpayers to tell them they owe money. Study respondents were asked if they had encountered such a scenario in the past 12 months and if so, did the encounter result in them spending money. If they answered “yes” to both questions, they were categorized as victims. If they answered “yes” to the first question and “no” to the second, they were categorized as “non-victims” (See Table 2,
pages 16-17, for a complete description of the scam scenarios and the estimated percentage of Americans encountering and experiencing a financial loss from each scam).

When asked about these 26 scams, nine out of ten respondents (91%) said they had encountered at least one of them in the past 12 months, which translates to over 229 million U.S. adults. Most experts attribute this high percentage of Americans encountering at least one incident of fraud to the explosion of robocalling in the United States. Robocall blocking firms encountered at least one incident of fraud 229 million U.S. adults. Most experts estimate that Americans receive 50 billion robocalls each year and almost half of these are fraudulent.22

The study also found that one in seven American adults (15%) or an estimated 33.5 million people spent money on at least one scam in 2020 (see Table 1). Additionally, Jury Duty (12%), Romance (12%), Miracle Medical Cure Products (11%), and Pain Relief Products (10%) were among the top five scams in which a financial loss resulted.

**Car warranty scams were, by far, the most prevalent scam encountered, with 175 million (70%) adults reporting having encountered the scam in the past year.**

**Table 1: Incidence of scam encounters and resulting financial losses, U.S. adults 18+**

<table>
<thead>
<tr>
<th>DEMOGRAPHIC SUBGROUP</th>
<th>TOTAL U.S. ADULT POPULATION</th>
<th>PERCENTAGE OF U.S. ADULT POPULATION</th>
<th>EXPERIENCED AT LEAST ONE SCAN ENCOUNTER</th>
<th>EXPERIENCED A FINANCIAL LOSS (AMONG THOSE ENCOUNTERING A SCAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>TOTAL U.S. ADULTS</td>
<td>PERCENTAGE OF U.S. ADULTS</td>
</tr>
<tr>
<td>Total</td>
<td>252,117,111</td>
<td>100.0%</td>
<td>229,069,435</td>
<td>90.9%</td>
</tr>
<tr>
<td>18-49</td>
<td>135,317,332</td>
<td>53.7%</td>
<td>122,608,309</td>
<td>90.6%</td>
</tr>
<tr>
<td>50+</td>
<td>116,799,779</td>
<td>46.3%</td>
<td>106,461,126</td>
<td>91.1%</td>
</tr>
</tbody>
</table>

**Chart 2: Top 10 Most Successful Scams in the Past Year**

- Notario: 24.0%
- Jury duty: 11.8%
- Romance: 11.5%
- Miracle medical cure products: 10.7%
- Pain relief products: 10.0%
- Government grant: 9.0%
- Grandparent: 9.0%
- IRS: 9.0%
- Weight loss products: 8.8%
- Corona vaccine: 8.7%

**Summary**

When it comes to how much fraud is out there, the bad news is that there is a lot. Not only has the number of fraud reports increased by 45% in 2020, but 229 million U.S. adults encountered at least one scam in 2020 and over 33.5 million people lost money. These data raise a fundamental question: how do the lives of the 33.5 million who lost money to fraud differ from the lives of 195.5 million others who encountered a scam and were able to resist?23

\*Note: For each of the 26 scams, their percentage of success was calculated by dividing the total number of adults who indicated spending money due to the scam by the total number of adults encountering the scam.
<table>
<thead>
<tr>
<th>Scam Type AND Ranking</th>
<th>% Encountering the Scam</th>
<th>% Experiencing a Financial Loss Due to the Scam</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Car Warranty</td>
<td>70.2% (175,517,824)</td>
<td>2.8% (7,069,154)</td>
</tr>
<tr>
<td>2. Tech Support</td>
<td>47.0% (117,750,073)</td>
<td>2.4% (6,082,547)</td>
</tr>
<tr>
<td>3. Social Security</td>
<td>42.7% (107,098,051)</td>
<td>2.2% (5,527,524)</td>
</tr>
<tr>
<td>4. Eliminate Credit Card Debt</td>
<td>41.2% (102,946,952)</td>
<td>1.9% (4,750,856)</td>
</tr>
<tr>
<td>5. Fake Job Offer</td>
<td>41.0% (102,656,654)</td>
<td>1.8% (4,505,191)</td>
</tr>
<tr>
<td>6. IRS</td>
<td>38.6% (96,819,865)</td>
<td>3.5% (8,671,366)</td>
</tr>
<tr>
<td>7. Weight Loss Products</td>
<td>35.1% (87,910,847)</td>
<td>3.1% (7,735,171)</td>
</tr>
<tr>
<td>8. Charity</td>
<td>35.1% (87,865,573)</td>
<td>2.7% (6,850,798)</td>
</tr>
<tr>
<td>9. Student Loan</td>
<td>34.6% (86,684,220)</td>
<td>1.7% (4,334,150)</td>
</tr>
<tr>
<td>10. Phishing</td>
<td>32.7% (81,767,642)</td>
<td>1.4% (3,476,857)</td>
</tr>
</tbody>
</table>

### TABLE 2: Incidence of Scam Encounters and Resulting Financial Losses, by Scam Type

*NOTE: See the Appendix, pages 44–45, for a detailed description of each scam scenario.

<table>
<thead>
<tr>
<th>Scam Type AND Ranking</th>
<th>% Encountering the Scam</th>
<th>% Experiencing a Financial Loss Due to the Scam</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. Foreclosure</td>
<td>30.7% (76,842,102)</td>
<td>1.4% (3,563,922)</td>
</tr>
<tr>
<td>12. Pain Relief Products</td>
<td>30.3% (75,713,370)</td>
<td>3.0% (7,557,039)</td>
</tr>
<tr>
<td>13. Lottery</td>
<td>29.2% (73,038,937)</td>
<td>1.6% (4,116,952)</td>
</tr>
<tr>
<td>14. Government Grant</td>
<td>24.6% (61,745,755)</td>
<td>2.2% (5,574,673)</td>
</tr>
<tr>
<td>15. Business Opportunity</td>
<td>23.6% (59,066,605)</td>
<td>1.2% (2,947,392)</td>
</tr>
<tr>
<td>16. Investment</td>
<td>23.6% (59,017,871)</td>
<td>1.3% (3,300,203)</td>
</tr>
<tr>
<td>17. Covid PPE (Personal Protective Equipment)</td>
<td>20.8% (51,820,472)</td>
<td>1.6% (3,958,155)</td>
</tr>
<tr>
<td>18. Timeshare Resale</td>
<td>16.4% (40,938,357)</td>
<td>1.3% (3,297,786)</td>
</tr>
<tr>
<td>19. Anti-Memory Loss Products</td>
<td>15.9% (39,799,237)</td>
<td>1.0% (2,493,307)</td>
</tr>
<tr>
<td>20. Romance</td>
<td>14.5% (36,331,197)</td>
<td>1.7% (4,176,926)</td>
</tr>
<tr>
<td>21. Covid Vaccine</td>
<td>12.2% (30,521,756)</td>
<td>1.1% (2,653,338)</td>
</tr>
<tr>
<td>22. Anti-Aging Products</td>
<td>12.1% (30,398,483)</td>
<td>1.0% (2,586,123)</td>
</tr>
<tr>
<td>23. Jury Duty</td>
<td>11.5% (28,760,941)</td>
<td>1.4% (3,389,244)</td>
</tr>
<tr>
<td>24. Grandparent</td>
<td>10.6% (26,508,325)</td>
<td>1.0% (2,381,690)</td>
</tr>
<tr>
<td>25. Miracle Medical Cure Products</td>
<td>9.0% (22,520,632)</td>
<td>1.0% (2,416,211)</td>
</tr>
<tr>
<td>26. Notario</td>
<td>4.9% (12,304,276)</td>
<td>1.2% (2,951,556)</td>
</tr>
</tbody>
</table>
WHAT MAKES US SUSCEPTIBLE TO FRAUD?

With nine in ten Americans being exposed to fraud each year and over 33.5 million consumers losing money, it has never been more important to understand when and why some people lose money while others are able to resist. The key to that understanding may lie in an analysis of how victims differ from non-victims on a range of environmental and social factors. The Fraud Frontiers Study asked all respondents questions designed to determine how victims may differ from non-victims in these areas. What emerged were three meta-factors that put us most at risk: emotion, environment, and exposure.

*The crush or the kill is emotionally driven. It’s not logic. If you apply logic to this concept, it’s no. I am not going to send you my hard-earned money. But when I wrap that in tons of emotion, that blurs everything.*

— JIM VITALE, CONVICTED SCAMMER (SHADEL, 2012)
META-FACTOR #1: EMOTION
The Impact of Emotional Arousal and Feelings of Control on Fraud Susceptibility

One of the most important areas explored in this study was the role that scammer’s manipulation of consumers’ emotions plays in fraud susceptibility. The origins of this line of inquiry started in the mid-2000s, when AARP researchers conducted qualitative interviews of over two dozen convicted scammers. The scammers were each asked, “What is your central strategy for scamming people?” The answer was always the same: “Get the victim under the ether.” Ether is scammer slang for a heightened emotional state where they can be more easily manipulated. As convicted con man Jim Vitale pointed out: “The crush or the kill is emotionally driven. It’s not logic. If you apply logic to this concept, it’s no. I am not going to send you my hard-earned money. But when I wrap that in tons of emotion, that blurs everything.”

A recent AARP educational video depicted undercover footage of a very skilled tech support scammer manipulating his target’s emotions. One minute he tells her, “You remind me of my grandmother who was my best friend.” The next minute he is blaming her, “This was YOUR mistake and as a result, I am going to be fired. Now what are you going to do about it?” The victim responds by saying, “I’m emotionally exhausted. Just tell me what you want me to do.”

Keeping victims off-balance, under the ether and out of control is a strategy almost all scammers employ because it can render our cognitive powers temporarily useless. At such moments, it doesn’t matter how much intelligence, education or success one has because the scammer has moved us away from logic to the point where our emotions are in charge. This may explain in part why it has been so difficult to find a single set of demographic characteristics that predict victimization. What victims may have in common is that they are simply human and therefore susceptible to temporarily allowing their emotions to get the better of them.

Cyber security researchers have found similar patterns when it comes to tracing the root causes of data breaches which lead to identity theft. Several studies suggest that 90% of all computer database breaches are the result of “social engineering” which is a fancy term for manipulating human emotions to defeat a computer’s defenses.

One example is tech support scams that use fear to gain the victim’s cooperation. The typical pitch begins with: “You have a dangerous virus on your computer, and you need to let us remote access in to fix it.” Here the scammer’s target may have state of the art anti-virus and firewall protection, but if they are persuaded through fear tactics that there is a virus on their machine, they unintentionally help the scammer bypass all of those defenses. As one of the pioneers of the dark web, convicted cyber scammer Brett Johnson told AARP researchers, “Sure I could spend several days hacking into someone’s system, but it’s much easier to call them up and scare them into voluntarily letting me in.”

A 2014 Stanford University study tested the ether theory and its role in fraud. Researchers brought subjects into a lab and asked them to play a rigged monetary incentive game. In the game, one third of the subjects lost money, which induced heightened negative emotion; one third gained money which induced heightened positive emotion; and one third broke even, which kept emotions neutral. Once these emotions were induced, subjects were asked to make financial decisions while “under the ether.” Significantly more of those in either a positive or negative heightened emotional state agreed to purchase products that were deceptively advertised compared to those kept in a neutral emotional state.

In the present study, respondents were asked, “To what extent did you feel any of the following emotions during your encounter?” Respondents were then given a list of ten emotions to choose from such as happy, excited, worried, or overwhelmed during their most recent scam encounter.

The working hypothesis underlying this question was that victims would report experiencing more and stronger emotions during fraud encounters than non-victims who were able to resist.

In fact, that is precisely what the data revealed. Far more victims than non-victims said they felt strong emotions during the fraud encounter. The only two areas where non-victims reported stronger emotions than victims were in response to the words “doubtful” and “angry” which makes sense given they both connote suspicion or hostility that would likely lead to resistance (see Chart 3).

It is important to note that victims experienced significantly more of both positive and negative emotions than non-victims. The most common of the positive emotions was “happy” which is the one the scammers use most often to overcome our resistance. The emotion most felt was “worried” which is probably the emotion we all feel the most when we are being scammed. It is also interesting that the vast majority of victims felt more of the negative emotions they were responding to than the non-victims did.”

— STEPHEN MICHAELS, CONVICTED SCAMMER (SHADEL, 2012)
negative emotions compared to non-victims (see Table 3). This finding is consistent with the Stanford study of heightened emotions and fraud which found that both negative and positive heightened emotions led to sub-optimal decision-making when confronted with malicious content.

It also explains why some scammers have told researchers they are just as happy talking to people who have lost hundreds of thousands of dollars to fraud already as they are to new potential victims. Convicted scammer Jim Vitale said, “If I know someone has already lost a lot of money, I just let them vent about how awful it was until they work themselves into a frenzy of emotion, and then I pitch them on how my deal is different.”

**FEELINGS OF CONTROL**

From a strategic perspective, the scammer’s goal is to get their target into a heightened emotional state so that they are easier to persuade and control. In fact, five times as many victims (33%) reported feeling out of control at the time of the fraud encounter compared to non-victims (6%) (see Chart 4).

In addition to self-reported emotions, respondents were also asked questions designed to get them to reflect on how they make decisions when in a heightened emotional state in general. Two of the questions related to positive emotional states (“I tend to lose control when I am in a great mood” and “I tend to act without thinking when I am excited”) and two of the questions related to negative emotional states (“When I am upset, I often act without thinking,” and “When I feel bad, I will often do things I later regret in order to feel better now”). More victims reported they are likely to make decisions without thinking or that they later regret when they are in a heightened emotional state, whether that emotional state is positive or negative (see Chart 5).

The survey also included the Arousal Predisposition Scale (APS), which is a peer-reviewed personality assessment designed to measure emotional arousability. The higher the score, the greater the arousability of the respondent. This personality measure was included in the study to determine if victims had more of a predisposition towards emotional arousability than non-victims which might increase their susceptibility to losing money to scams.

In fact, on average, victims did score significantly higher (32.1) on the Arousal Predisposition Scale than non-victims (30.5). Additionally, victims were more likely to report frequently, almost always or always doing more of each individual behavior than non-victims (see Chart 6).

**TABLE 3: THE AVERAGE NUMBER OF EMOTIONS EXPERIENCED DURING THE SCAM ENCOUNTER**

<table>
<thead>
<tr>
<th></th>
<th>VICTIMS (n = 1085)</th>
<th>NON-VICTIMS (n = 2173)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AMONG THE 5 POSITIVE EMOTIONS</strong></td>
<td>3.04</td>
<td>0.59</td>
</tr>
<tr>
<td><strong>AMONG THE 5 NEGATIVE EMOTIONS</strong></td>
<td>3.36</td>
<td>2.07</td>
</tr>
</tbody>
</table>

**CHART 4: THE PERCENTAGE REPORTING FEELING OUT OF CONTROL**

<table>
<thead>
<tr>
<th></th>
<th>VICTIMS (n = 1085)</th>
<th>NON-VICTIMS (n = 2173)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am a calm person*</td>
<td>61%</td>
<td>68%</td>
</tr>
<tr>
<td>I can be emotionally moved by what other people consider to be simple things</td>
<td>25%</td>
<td>19%</td>
</tr>
<tr>
<td>I find that my heart keeps beating fast for a while after I have been stirred up</td>
<td>25%</td>
<td>19%</td>
</tr>
<tr>
<td>Strong emotions carry over for one or two hours after I leave the situation which caused them</td>
<td>25%</td>
<td>22%</td>
</tr>
<tr>
<td>I get flustered when I have several things to do at once</td>
<td>24%</td>
<td>20%</td>
</tr>
<tr>
<td>I startle easily</td>
<td>21%</td>
<td>15%</td>
</tr>
<tr>
<td>My mood is quickly influenced by entering new places</td>
<td>21%</td>
<td>13%</td>
</tr>
<tr>
<td>I tend to remain excited or moved for a long period of time after seeing a good movie</td>
<td>19%</td>
<td>19%</td>
</tr>
<tr>
<td>I am easily frustrated</td>
<td>13%</td>
<td>13%</td>
</tr>
<tr>
<td>I am restless and fidgety</td>
<td>14%</td>
<td>18%</td>
</tr>
<tr>
<td>Sudden changes of any kind produce an immediate emotional effect on me</td>
<td>18%</td>
<td>13%</td>
</tr>
<tr>
<td>I get excited easily</td>
<td>11%</td>
<td>11%</td>
</tr>
</tbody>
</table>

*NOTE: This item is reverse-coded.

**CHART 5: MAKING DECISIONS UNDER HEIGHTENED EMOTIONS (PERCENTAGE AGREEING SOMEWHAT OR STRONGLY)**

<table>
<thead>
<tr>
<th></th>
<th>VICTIMS (n = 1085)</th>
<th>NON-VICTIMS (n = 2195)</th>
</tr>
</thead>
<tbody>
<tr>
<td>When I am upset, I often act without thinking</td>
<td>44%</td>
<td>32%</td>
</tr>
<tr>
<td>When I feel bad, I will often do things I later regret in order to feel better now</td>
<td>26%</td>
<td>39%</td>
</tr>
<tr>
<td>When I am upset, I often act without thinking</td>
<td>24%</td>
<td>27%</td>
</tr>
</tbody>
</table>

**CHART 6: EMOTIONAL AROUSABILITY SCALE (PERCENTAGE REPORTING THE STATEMENT DESCRIBES THEM FREQUENTLY, ALMOST ALWAYS OR ALWAYS)**
SUMMARY
The data in this survey are some of the strongest evidence we have seen to date that shows the relationship between strong emotions and fraud susceptibility. Not only do victims report significantly more and stronger emotions at the time of fraud encounters, but significantly more victims report feeling out of control during these encounters, which is precisely the goal of the scammer. In addition, more victims report making decisions they later regret when in a heightened emotional state and more victims score significantly higher on the Arousal Predisposition Scale than non-victims. All of these data combine to reinforce the importance of consumer education regarding scammers’ chief goal of increasing their targets’ emotional arousal during a fraud encounter. Increasing their targets’ emotional arousal makes the scammer’s job that much easier, and the chances of their targets losing money, that much greater.

META-FACTOR #2: ENVIRONMENT
The Impact of Stressful Life Events on Fraud Susceptibility

Previous research has shown that one’s environment can have a powerful impact on fraud susceptibility. For example, studies have found a correlation between fraud victimization and stressful life events. The Fraud Frontiers Study data replicated this finding in a powerful way. Respondents were presented with 17 stressful life events such as illness, death of a loved one, loss of a job, and loneliness, and were asked to indicate all of those they had experienced in the past 12 months (see Chart 7). Victims reported experiencing twice as many stressful life events (4.0) on average as non-victims (1.9) (see Chart 8).

The theoretical explanation for this correlation between life stress and victimization goes like this: coping with stress consumes cognitive capacity that might otherwise be used to spot and resist a fraud attempt. The Fraud Watch Network Helpline staff and volunteers have anecdotally known about this correlation for many years. Many people will call to report that they have experienced a scam, but the scam is rarely the only life situation they describe or are involved in.

“It’s not at all uncommon for a victim to contact us about a romance scam or a tech support scam they encountered, but then start talking about several other difficult issues they are dealing with,” said Amy Nofziger, Director of Fraud Victim Support for AARP’s Fraud Watch Network.

And we know from analyzing thousands of conversations between scammers and victims that the scammer will intentionally probe for the presence of such stressful life events and when the potential victim reveals a recent divorce or illness, scammers will focus the victim’s attention on that event to keep them off balance and drain even more of their cognitive power.

“I would ask the fraud target to tell me their life story so I could find their emotional Achilles heel” said Stephen Michaels, a convicted investment fraud scammer during an interview with AARP researchers. “Once I found it, I would throttle up on that event by saying, ‘Tell me more about your husband’s illness.’”

CHART 8: STRESSFUL LIFE EVENTS EXPERIENCED AT THE TIME OF THE SCAM ENCOUNTER

CHART 7: AVERAGE NUMBER OF STRESSFUL LIFE EVENTS EXPERIENCED IN PAST 12 MONTHS
Anyone who has interviewed individuals who have lost money to a romance scam can attest to the presence of other stresses in their lives. AARP researchers interviewed a former romance scammer named Enitan several years ago and asked, “How many of your victims had experienced some kind of loss in the previous year?” “Every single one of them” was his answer. The dating sites he frequented to target his victims were filled with lonely people who had recently lost a spouse or a loved one. When asked what made them susceptible to his scams, he said, “A lonely heart is a vulnerable heart.” This study also found that victims (33%) were more than twice as likely as non-victims (13%) to report feeling lonely in the past year.

Another set of important environmental factors that can impact susceptibility to fraud is health and finances. The survey found victims reported more health and financial issues than non-victims:

- More victims (24%) reported that they have fair or poor health than non-victims (19%).
- More victims (32%) reported that they frequently or sometimes require assistance remembering appointments, family occasions, holidays, or taking medications than non-victims (23%).
- In addition, when asked about their changing financial situation, more victims reported a decline in their financial situation than non-victims:
  - More victims (40%) reported that their financial situation has gotten worse since the coronavirus pandemic started in January 2020 than non-victims (27%).
  - More victims (30%) said their debt is far more or a bit more than they can handle financially than non-victims (20%).

SUMMARY

The role of one’s changing environment on fraud susceptibility is in full view in this study, with victims experiencing twice as many stressful life events as non-victims, as well as declining health and finances. These findings suggest that coping with such environmental changes may impact one’s ability to spot and resist fraud. It may also influence the extent and ease with which the scammer can work the target of the scam into a heightened emotional state because many of us can get emotional dealing with the death of a family member or the loss of a job. Add to this the scammer’s ability to probe for such events and then focus the victim’s attention on it and you have a dangerous combination that can lead to exploitation.

META-FACTOR #3: EXPOSURE

The Impact of Certain Actions on Exposure to Scams

As part of the Fraud Frontiers Study, all respondents were asked to report the total number of fraud encounters they had in the previous 12 months. Victims reported having encountered 58% more fraud attacks on average (11.5) compared to non-victims (7.3) (see Chart 9).

There could be several explanations for why victims experienced so many more scam encounters compared to non-victims. One explanation is that once a person has responded to a scam, they are placed on lead lists that guarantee more calls from other scammers. Another possible explanation may lie in the fact that victims are more open to sales situations compared to non-victims.

The Fraud Frontiers Study asked respondents a series of questions to measure their openness to various sales situations like watching the home shopping channel, entering free drawings, listening to telemarketers, and opening and reading junk mail (see Chart 10, page 28). Respondents were also asked questions about their purchasing behavior such as the frequency with which they purchased products from previously unknown sellers or in response to TV ads or popup solicitations. The result was that victims were significantly more open to all of the sales situations they were asked to respond to in the survey and engaged in more activities that could result in a scam experience than non-victims.

RISK-TAKING & SENSATION-SEEKING

Respondents also were asked a series of questions designed to quantify attitudes towards risk-taking and what social psychologist Marvin Zuckerman termed “sensation-seeking,” the extent to which some people engage in activities just for excitement or to have new experiences. The sensation seeking scale was originally developed as a measure to predict risk-taking and substance abuse among teenagers and young adults, but it has been applied to many other populations since then. More recently, neuroscientists have used the sensation seeking scale and functional magnetic resonance imaging (fMRI) technology to show that individuals who score high on sensation-seeking are also more likely to activate the emotion centers of the brain when presented with stimuli.

The results showed victims score significantly higher than non-victims when it comes to their attitudes towards risk-taking and seeking exciting activities (see Chart II, page 28). Of particular note: significantly more victims than non-victims agreed with the statement, “I enjoy taking risks.” These findings, combined with respondent attitudes towards openness to the marketplace and activities that could lead to scams, may explain in part why victims reported experiencing so many more fraud encounters than non-victims.
SUMMARY

A third major set of risk factors revolves around exposure. Significantly more victims experienced multiple exposures to fraud and many of them demonstrated engaging in activities that may have caused some of that additional exposure such as being more open to solicitations from strangers and making remote purchases at a pace that significantly exceeded non-victims.

OTHER RISK FACTORS

In addition to the three E’s (Emotion, Environment, and Exposure), the Fraud Frontiers Study also looked at several potential socioeconomic and demographic risk factors. The findings show:

- More victims (63%) earned under $50,000 a year than non-victims (55%).
- More victims (44%) had a high school diploma or less education than non-victims (37%).
- More victims (57%) were ages 18–49 than non-victims (53%).
- More victims (15.4) score higher on a scale that measures the perceived importance of material wealth than non-victims (14.4).

While 11% of non-Hispanic White adults lost money to fraud, 22% of Non-Hispanic Black adults and 22% of Hispanic adults lost money to fraud.

These factors, however, may serve as proxies for actual underlying risk factors. In Part Four, What Risk Factors Best Predict Fraud Susceptibility, there will be a description of statistical tests that were run to determine which of the various risk factors were most influential in predicting financial loss due to a scam.

CHART 10: COMMON CONSUMER ACTIVITIES THAT MAY INCREASE OUR SUSCEPTIBILITY TO FRAUD (PERCENTAGE REPORTING DOING THE ACTIVITIES SOMETIMES OR FREQUENTLY)

<table>
<thead>
<tr>
<th>Activity</th>
<th>Victims (%)</th>
<th>Non-Victims (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used a peer-to-peer platform to send money to a family member or close friend</td>
<td>50</td>
<td>44</td>
</tr>
<tr>
<td>Opened and read every piece of mail you received, including advertisements</td>
<td>44</td>
<td>44</td>
</tr>
<tr>
<td>Entered your name in a drawing to win a free prize or gift</td>
<td>29</td>
<td>41</td>
</tr>
<tr>
<td>Purchased a product or service in response to an ad you saw on television</td>
<td>15</td>
<td>34</td>
</tr>
<tr>
<td>Used a peer-to-peer platform to send money to an individual seller (not a retailer) with whom you had not previously done business</td>
<td>19</td>
<td>32</td>
</tr>
<tr>
<td>Purchased a product or service in response to a pop-up or ad on a social media website like Facebook, from a company or individual with whom you had not previously done business</td>
<td>14</td>
<td>32</td>
</tr>
<tr>
<td>Watched the home shopping channel, QVC, or other shop at home TV shows</td>
<td>13</td>
<td>27</td>
</tr>
<tr>
<td>Gave out personal information to qualify for a free or discounted product or service</td>
<td>11</td>
<td>24</td>
</tr>
<tr>
<td>Purchased a product or service in response to an email you received from a company or individual with whom you had not previously done business</td>
<td>8</td>
<td>23</td>
</tr>
<tr>
<td>Called a toll-free number or ordered free information, such as CDs, books, or other promotional materials you heard advertised</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Listened to a telemarketer when they called to deliver a sales pitch over the phone</td>
<td>7</td>
<td>16</td>
</tr>
<tr>
<td>Purchased a product or service in response to a phone call you received from someone with whom you had not previously done business</td>
<td>4</td>
<td>15</td>
</tr>
</tbody>
</table>

VICTIMS (n = 1085)  NON-VICTIMS (n = 2195)

CHART 11: RESPONDENT ATTITUDES TOWARD RISK-TAKING AND SEEKING EXCITING ACTIVITIES (PERCENTAGE AGREEING STRONGLY OR SOMEWHAT)

<table>
<thead>
<tr>
<th>Attitude</th>
<th>Victims (%)</th>
<th>Non-Victims (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I enjoy taking risks</td>
<td>45</td>
<td>31</td>
</tr>
<tr>
<td>I like doing things just for the thrill of it</td>
<td>40</td>
<td>34</td>
</tr>
<tr>
<td>I like to have new and exciting experiences, even if they are a little frightening, unconventional, or illegal</td>
<td>37</td>
<td>37</td>
</tr>
<tr>
<td>I prefer friends who are excitingly unpredictable</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>24</td>
</tr>
</tbody>
</table>

VICTIMS (n = 1085)  NON-VICTIMS (n = 2195)
PART THREE: WHICH PROTECTIVE FACTORS MIGHT IMPACT OUR SUSCEPTIBILITY TO FRAUD?

The Fraud Frontiers Study addressed four key areas of protective factors that limit the likelihood of a scam’s success: family support networks; social support networks; technology protections like using a password manager, call blocking services, and identity theft monitoring services; and consumer education.

FAMILY SUPPORT NETWORKS
Respondents were asked a series of questions about the extent to which they have family members whom they can rely on to get advice and support as a preventative tool. This is an especially important area to probe because so many victims in previous studies have reported feelings of loneliness and isolation. A 2014 AARP study found that internet fraud victims are more likely than non-victims to report experiencing loneliness, feeling left out, or isolated from other people. A 2017 AARP study of military fraud victims and non-victims found that
victims were more likely to report feeling lonely and having family or relationship problems.\textsuperscript{32}

The theory underlying this series of questions was that victims might have less family support than non-victims and that lack of support could increase their susceptibility to fraud. In fact, the data shows that in every aspect of family support addressed by the survey, victims reported having less family support than non-victims (see Chart 12).

**SOCIAL SUPPORT NETWORKS**

The study pursued a similar line of reasoning in asking questions about the levels of social support experienced by victims and non-victims. Six different aspects of social support were included in the survey: help finding a job, knowing where to go for help when confronted with financial challenges, where to turn for food or housing, who to talk to when undergoing a crisis or when lonely, and having others who will listen to their problems.

Here there was once again clear evidence that victims had less social support than non-victims. On the three questions relating to support during a crisis or to discuss problems, victims reported having less support than non-victims. Similarly, on the three questions relating to where to go for financial help, fewer victims reported they had a place to go to get help (see Chart 13).

**OTHER PROTECTIVE FACTORS**

Respondents were asked about other protective factors to learn whether they may have helped to guard against fraudulent attacks. Specifically, eight questions were asked:

- Are they signed up for the National Do Not Call Registry?
- Do they subscribe to an ID theft monitoring service?
- Have they frozen their credit?
- Do they use a robocall blocking service?
- Do they have any protective software installed or enabled on their devices or computers?
- Do you they use a passcode, password, facial identification, or fingerprint recognition to unlock their devices or computers?
- Do they use a password manager to store and manage their online passwords?
- Do they use a distinctly different password for each of their online accounts?

The theory underlying these questions is that victims would have taken fewer precautions when it comes to basic technology related to fraud prevention.
protections than non-victims. However, in four of the eight areas probed by the survey, victims were significantly more likely than non-victims to use a robocall blocking service, subscribe to an ID theft monitoring service, have a credit freeze on credit accounts but not with all three major credit bureaus, and use a distinctly different password for all accounts (see Chart 14). Notably, the only areas where non-victims reported taking more precautions than victims were using a passcode on their computer and signing up for the National Do Not Call Registry.

**SUMMARY**

The role of protective factors in fraud susceptibility had some interesting results. The first hypothesis was victims would report having less family support and social support than non-victims, which may have contributed to their susceptibility to fraud. In fact, the data supports this assertion on all eleven measures addressed by the survey.

A second hypothesis was victims would report using fewer protective factors like robocall blocking, ID theft monitoring, and freezing credit. However, in four of the eight areas probed, significantly more victims reported using protective factors compared to non-victims. One explanation for this mix of results is that the survey did not delineate between taking protective action before a fraud encounter versus after a fraud encounter. So, it could be that more victims took protective action than non-victims because they had already been victimized and, therefore took those protective actions to avoid future victimization.

Perhaps more significantly, the data shows that only two of the eight protection tools recommended by fraud experts — using a passcode and installing protective software on one’s computer — were used by most respondents, regardless of victim status. And less than 50% of all respondents signed up for a robocall blocking app or the Do Not Call list which together can dramatically reduce exposure to scam encounters. Such exposure may not be a problem during normal day-to-day living, but if one is coping with a stressful life event such as an illness or loss of a job, or if one tends to become emotionally aroused by such encounters, limiting exposure to such malicious messages can be a vital prevention tool. More work needs to be done to encourage consumers to employ these essential prevention tools in the future.

---

**CHART 14: PROTECTIVE FACTORS EMPLOYED**

<table>
<thead>
<tr>
<th></th>
<th><strong>VICTIMS (n = 1085)</strong></th>
<th><strong>NON-VICTIMS (n = 2195)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a passcode or password, facial identity, or fingerprint recognition or unlock devices, or computer</td>
<td>85%</td>
<td>89%</td>
</tr>
<tr>
<td>Have protective software installed or enabled on devices or computers</td>
<td>74%</td>
<td>79%</td>
</tr>
<tr>
<td>Signed up for the National Do Not Call Registry</td>
<td>42%</td>
<td>51%</td>
</tr>
<tr>
<td>Use a password manager to store and manage your online passwords</td>
<td>41%</td>
<td>40%</td>
</tr>
<tr>
<td>Use a robocall blocking service</td>
<td>40%</td>
<td>33%</td>
</tr>
<tr>
<td>Subscribe to an ID theft monitoring service</td>
<td>29%</td>
<td>24%</td>
</tr>
<tr>
<td>Have a credit freeze on your credit accounts at at least one of the three major credit bureaus</td>
<td>24%</td>
<td>13%</td>
</tr>
<tr>
<td>Use a distinctly different password for each account</td>
<td>23%</td>
<td>18%</td>
</tr>
</tbody>
</table>
The report thus far has provided a description of many of the individual findings in the AARP Fraud Frontiers Study. However, more powerful statistical analyses were conducted by AARP researchers. The study included nearly 40 variables that might impact fraud susceptibility. A logistic regression analysis was run among the overall sample to determine which of these variables had the strongest predictive power when it comes to fraud. (See the Appendix, page 46, for a statistical summary.) These variables included numerous socioeconomic factors. The findings showed that socioeconomic variables like age, income and education, while numerically different in some instances, were not significant predictors in the regression.
The top four risk factors that predict fraud susceptibility all centered around the fraud encounters themselves: the total number experienced and the emotions felt during those encounters:

- Positive emotions felt during the fraud encounter such as happy, hopeful, excited, adventurous and/or lucky
- Total number of scam encounters
- Feeling out of control during encounter
- Negative emotions such as worried, overwhelmed, intimidated and/or angry felt during the encounter

Strong positive emotions experienced during the fraud encounter was the strongest predictor by a factor of more than two to one over any other variable. The total number of encounters was the second most predictive variable, which stands to reason because it is a measure of total exposure to the persuasion tactics of the scammers and victims reported having 60% more encounters than non-victims. This was followed by feeling out of control during a fraud encounter, which makes sense because the data shows five times as many victims reported feelings of being out of control during the fraud encounter compared to non-victims. The presence of negative emotions during a fraud encounter rounds out the top four.

The fact that positive emotions, negative emotions, and feeling out of control represent three of the top four influences also reinforces that emotional arousability is a critical variable driving whether one loses money or is able to resist a fraud encounter.

The top two factors that significantly decreased fraud susceptibility were:
- Extent to which feeling doubtful was experienced during a scam encounter
- Positive change in financial situation since the coronavirus pandemic started

Feeling doubtful obviously is an emotion that would make it more likely that the person encountering a fraud would resist given they have some skepticism about the offer. A positive change in one’s financial situation ostensibly decreases the need to make money which may explain the reduced chances of fraud susceptibility.

CONCLUSION

The AARP Fraud Frontiers Study found that over 33 million Americans (15% of the population) lost money to fraud in 2020. The enormity of the fraud problem has given rise to the need to critically address and understand when and why some people are more susceptible to fraud.

The result of this research was the identification of several key factors that predict fraud susceptibility.
1. **Fraud Prevention Education Should Include Building Awareness of the Role Stress and Emotional Arousal Play in Fraud Susceptibility.**

These new findings have implications for fraud prevention programming in the future. In the past, we focused so much energy on providing cognitive tools for avoiding fraud: teaching persuasion tactics, offering checklists of things to investigate before buying, etc. However, very little has been done to increase the awareness that stressful life events and heightened emotions weaken our defenses to scams. Previous studies have shown that consumer education is a deterrent to victimization. We should develop new content that addresses these two key risk factors and teach consumers about the idea of the “susceptible moment.” This content could focus on the idea of “notice the moment” to raise awareness of the role our immediate environment and our reaction to it plays in fraud susceptibility. After all, the scammer’s goal is to knock us off that solid cognitive foundation and into the murky and unpredictable world of passion and emotional reactivity. It will be important to help consumers recognize the potential susceptibility that comes with emotional arousability, given the reality that a person’s emotional makeup isn’t something education is likely to change.

2. **Protective Factors That Limit Exposure to Scams Should Be Encouraged.**

Because victims experienced 60% more fraud encounters than non-victims, we should encourage protective services that limit exposure to fraud such as: call blocking, credit freezes, online monitoring of accounts, password management, closing out online accounts not in use, etc. AARP should continue to look for opportunities to partner with companies or organizations that can help in this regard and should also redouble our efforts to police our own marketing and advertising to 38 million members to ensure that we are not unwittingly exposing them to malicious content.

In addition, developing an early warning system that can spot fraud when it first emerges in a community might help consumers resist malicious attempts. AARP hopes to work with the private sector to help develop such a system.

3. **Social and Family Support Systems Can Reduce Fraud Susceptibility.**

One of the important findings of this study was the role that social isolation and a relative lack of social and family support may play in fraud victimization. The study found victims reported more experiences of loneliness and less social and family support than non-victims. These data support years of anecdotal reports from fraud prevention experts that so many fraud victims were socially isolated when exposed to and victimized by fraud. We need to think creatively about ways to better connect with AARP members to reduce this risk factor.

4. **Continue the Theme That Fraud Can Happen to Anyone.**

This research shows that no one demographic characteristic is the primary source of fraud susceptibility. An individual can have a PhD in psychology, be a millionaire or a senior partner in a law firm and still lose money to scams. Yet there continues to be stereotypes and labels placed on many victims. AARP and fraud prevention professionals need to keep promoting the message that fraud can happen to anyone given the right scammer and the right moment in time because a) it’s true and b) it requires everyone to be on guard to defend against such scams. If consumers think that older people, uneducated people, low-income people, or some select ‘others’ are the only ones susceptible to fraud, that may give them a false sense of security, which paradoxically can lead to greater susceptibility.
AARP commissioned NORC in July 2020 to examine rates of encounters and financial loss from 26 types of scams among a general population of U.S. adults ages 18 and older. The sample was selected from NORC’s AmeriSpeak® Panel, a probability-based panel designed to be representative of the U.S. household population.

Notably, the survey respondents were not informed that the 26 scams were “scams.” Instead they were described as “scenarios that are seen in the marketplace.” Those indicating that they were exposed to one or more of the 26 scams met the initial screening criteria and were asked an additional set of questions. Additionally, those who indicated that they spent money as a result of the scenario were classified as having experienced a financial loss from a scam.

A total of 3,280 interviews, including oversamples of 739 Black/African American respondents and 704 Hispanic/Latino respondents, were completed. Among the total sample, 1,085 experienced a financial loss from a scam and 2,195 did not experience financial loss from a scam.

Data collection for the study began on October 26, 2020 and continued through November 17, 2020. The survey was fielded in English and Spanish. The overall margin of sampling error is +/- 2.52 percent. Weighting was calculated using panel base sampling weights to start. Panel weights are raked to external population totals associated with age, sex, education, race/Hispanic ethnicity, housing tenure, telephone status, and Census Division. The external population totals are obtained from the Current Population Survey. The weights adjusted to the external population totals are the final panel weights.

For technical information about the AmeriSpeak® Panel, including recruitment process and panel management policies, please see www.aarp.org/momentsnotice.

### POTENTIAL LIMITATIONS

1. Recall of Past Events. Because respondents were asked to recall being exposed to various encounters during the past 12 months, the accuracy of their responses is questionable. Past studies have shown that events that occur more than three months ago, an outcome of an event, or emotionally arousing events, may impact one’s ability to accurately recall a specific event or experience. Age may also influence recall accuracy.

2. Additional Context. Due to the survey length, some questions were not included that in retrospect would have been beneficial to the study.

At the end of the survey, respondents were not asked whether they had ever lost money to a scam, whether they thought the encounter they experienced was a scam, or when the encounter occurred (e.g., a month ago, 2-3 months ago, 4-5 months ago or more than 6 months ago). Because the word “scam” was not used, this would have been helpful in determining whether the respondents who indicated spending money on a scam encounter knew that the encounter in which they spent money was a scam.

In addition, asking respondents who spent money as a result of a scam when they instituted protective measures to safeguard their accounts and devices, either before or after they spent money (i.e., experienced a financial loss from a scam), would have answered whether these measures were purely preventative or reactive (i.e., employed after their financial loss to keep something like this from happening again).
APPENDIX

SCAM SCENARIO DESCRIPTIONS

APPENDIX A

1. CAR WARRANTY: Someone contacts you and tells you that your car warranty is about to expire, and they can help you get a good deal on an extension of that warranty. They ask you to provide some personal information (e.g., credit card number, Social Security number, Driver’s license number).

2. TECH SUPPORT: Someone contacts you saying there is a virus on your computer, or you have a software license that needs to be renewed and you need to act right away.

3. SOCIAL SECURITY: Someone contacts you saying your Social Security number has been compromised or that you owe money and must act right away to straighten things out.

4. ELIMINATE CREDIT CARD DEBT: Someone contacts you or you see an advertisement about helping you get rid of thousands of dollars of credit card debt. The fee for their assistance, however, must be paid in advance.

5. FAKE JOB OFFER: Someone contacts you or you see a job listing offering opportunities to work at home, be a mystery shopper, or some other “too good to be true” sounding job. The job usually involves paying an upfront fee — providing your credit card or bank account information.

6. IRS: Someone calls you on the phone saying they work for the IRS and that you owe the IRS money.

7. WEIGHT LOSS PRODUCTS: Someone contacts you about a weight-loss product they guarantee will help you lose weight fast and still eat all you want.

8. CHARITY: Someone contacts you or you see an advertisement to donate money to a worthy cause (like supporting animal rescue, fighting homelessness, or providing aid after a high-profile disaster). They ask for donations to be in cash, by gift card, or by wiring money. You do not have a prior relationship with the charity.

9. STUDENT LOAN: Someone contacts you offering quick relief from your federal student loans or warning that the student loan forgiveness programs will end soon. To assist you, they may require that you pay an up-front fee, provide your Federal Student Aid ID and/or provide them permission to speak to your federal loan servicer on your behalf.

10. PHISHING: Someone contacts you saying they are from your bank or another business with which you have a relationship stating there is something wrong with your account and asking you to provide personal information (e.g., date of birth, Social Security number, bank account information) to verify the account.

11. FORECLOSURE: Someone contacts you or you see an advertisement from a company stating they can reduce your mortgage payments. They may charge you a large up-front fee, tell you not to pay your mortgage, or request that you send your title or payments to them.

12. PAIN RELIEF PRODUCTS: Someone offers a product that is guaranteed to reduce the various pain you might have in shoulders, back, knees, etc. that you can buy without a prescription.

13. LOTTERY: Someone contacts you saying you won money from a lottery or some other type of prize, but you must pay taxes, a fee, or other money to receive the winnings or the prize.

14. GOVERNMENT GRANT: Someone contacts you or you see an advertisement about “free government grants” worth thousands of dollars. To receive these grants or to determine your eligibility, you are asked to provide your bank account information (so they can deposit your grant directly into your account or cover a one-time processing fee). You are assured that you can get a refund if you are not satisfied.

15. BUSINESS OPPORTUNITY: Someone contacts you or you see an advertisement that offers to help you start your own business — offering high pay in a short period of time for very little effort. The products you would sell may be low-quality, cheap, or outdated merchandise.

16. INVESTMENT: Someone contacts you or you see an advertisement guaranteeing that you will receive a high rate of return on an investment — with little or no risk. This could be selling oil and gas, gold coins, real estate, deeds of trust, etc.

17. COVID PERSONAL PROTECTION EQUIPMENT: Someone contacts you or you see an advertisement about having access to free face masks or hand sanitizers to protect against the spread of the coronavirus.

18. TIMESHARE RESALE: Someone contacts you or you see an advertisement for a product or service that guarantees you will not lose your memory or get Alzheimer’s disease.

19. ANTI-MEMORY LOSS PRODUCTS: Someone contacts you or you see an advertisement for a product that guarantees you will not lose your memory or get Alzheimer’s disease.

20. ROMANCE: Someone contacts you on a dating site or app pretending to have romantic intentions to gain access to your money, credit cards, property, or identification information.

21. COVID VACCINE: Someone contacts you or you see an advertisement about a vaccine for the coronavirus that you can get or purchase.

22. ANTI-AGING PRODUCTS: Someone contacts you about a revolutionary new medicine that they guarantee will add years to your life.

23. JURY DUTY: Someone contacts you saying that you missed jury duty and there is a warrant out for your arrest. They tell you that, to avoid being arrested, you will need to pay a fine.

24. GRANDPARENT: Someone contacts you pretending to be your grandchild or other family member — or claims to represent your grandchild or family member (e.g., a lawyer or law enforcement agent). They ask you to send them money to help with an emergency, pay for bail, or pay an unexpected bill, etc.

25. MIRACLE MEDICAL CURE PRODUCTS: Someone contacts you about a product they guarantee will help you become cancer-free and will miraculously cure other ailments and diseases.

26. NOTARIO: Someone contacts you or you see an advertisement that strongly implies they are a “notario” who is authorized to practice immigration law and can guarantee to help move your immigration papers forward for an upfront fee.

NOTE: For each of the 26 scams, their percentage of success was calculated by dividing the total number of adults who indicated spending money due to the scam by the total number of adults encountering the scam.
LOGISTIC REGRESSION ANALYSIS DATA

**ALL RESPONDENTS (n = 1,786)**

<table>
<thead>
<tr>
<th>B</th>
<th>S.E.</th>
<th>Wald df Sig. Exp(B)</th>
<th>Exp(B) Upper</th>
<th>Lower</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.579</td>
<td>0.096</td>
<td>270.840 1 0.000 4.852</td>
<td>4.020 5.856</td>
<td></td>
</tr>
</tbody>
</table>

**Total number of scams encountered (0-26)**

| 0.623 | 0.076 | 67.540 1 0.000 1.865 | 1.607 2.164 |

**Extent to which respondent felt out of control during the encounter (0-3)**

| 0.575 | 0.039 | 33.819 1 0.000 1.778 | 1.464 2.158 |

**Extent to which respondent felt out of 4 negative emotions (i.e., worried, overwhelmed, intimidated and/or angry) during a scam encounter (0-12)**

| 0.477 | 0.103 | 21.296 1 0.000 1.612 | 1.316 1.974 |

**Age**

| 0.398 | 0.092 | 18.711 1 0.000 1.489 | 1.243 1.783 |

**Typically learning about the last consumer scams from one's bank or credit union**

| 0.394 | 0.165 | 5.695 1 0.001 1.484 | 1.073 2.051 |

**How respondent’s financial situation has changed since COVID. (1-worse, 2-same, 3-better)**

| -0.385 | 0.080 | 22.980 1 0.000 0.680 | 0.581 0.796 |

**Marital status: married**

| 0.698 | 0.228 | 9.372 1 0.000 1.489 | 1.285 1.756 |

**Marital status: separated/divorced/widowed**

| 0.413 | 0.275 | 2.247 1 0.134 1.511 | 0.881 2.591 |

**Constant**

| -1.080 | 0.210 | 88.750 1 0.000 0.138 |

ENDNOTES

2. FTC Consumer Sentinel, 2020
3. Personal conversation with Assistant US-Attorney
4. Franklin, 2003
5. AARP, 2005
7. Burke, Delima, 2019
8. Prevention in Webbank, Germany, 2009
9. Consumer Fraud Research Group, 2006
10. AARP, 2014
11. AARP, 2014
13. AARP, 2011
14. Castle, 2017
15. AARP, 2011
16. FTC, 2013, FTC, 2019
17. Consumer Fraud Research Group, 2006
19. Pratkanis, 2005
20. AARP Scam Alert Bookazine, 2017
22. YouMail Annual Report 2019
23. FTC, 2013, FTC, 2019
24. Lovemore, 2016
26. Interview with Brett Johnson, 2018
27. Kirknald, 2018
28. AARP, 2014, FTC, 2019
30. FRIENDS National Center for Community Based Child Abuse Prevention, 2021
31. AARP, 2014
32. NHAC, 2010
33. AARP, 2011, FTC, 2013, FTC, 2019
34. Howard, 2011
35. Rhodes, 2019

APPENDIX B

REFERENCES


AARP (2014) Caught in the Scammers’ Web: Factors that May Lead to Becoming a Victim of Internet Fraud. (Karla Pak, Doug Shadel and Jennifer Sauer) Washington, DC.


Howard, B.H. Testing the accuracy of the retrospective recall method used in expertise and spoofing. (Alice Williams, Jennifer Sauer, Karla Pak and Doug Shadel) Washington DC.

The YouMail Robocall Index, located at: https://robocallindex.com


YouMail Robocall Index, located at: https://robocallindex.com

A Moment’s Notice

Recognizing the Stressful Life Events, Emotions and Actions that Make Us Susceptible to Scams:

An AARP National Fraud Frontiers Report

www.aarp.org/momentsnotice