2017 BBB Scam Tracker Annual Risk Report:
New Trends in Scam Risk
The Better Business Bureau Institute for Marketplace Trust (BBB Institute) is proud to publish its second annual BBB Scam Tracker Annual Risk Report. As the charitable education and research arm of the Better Business Bureau (BBB), we create and deliver educational programs, guidelines, and research that foster a trustworthy marketplace in which consumers and businesses can prosper. We teach consumers how to avoid scams, establish best practices and ethical standards for businesses, and develop new strategies and programs to address barriers to an accessible, fair, and safe digital marketplace.

BBB Scam Tracker™ was developed thanks to a grant provided to the BBB Institute in 2015 to address a need identified by local Better Business Bureaus for an easy-to-use online tool to empower consumers to report scams in real time. Using consumer reports, this online tool collects and shares robust and timely data that shed light on how scams are being perpetrated, who is being targeted, which scams have the greatest impact, and much more. A healthy marketplace needs empowered and aware consumers and principled businesses that are proactively working to stop scammers. Scam Tracker provides the crowdsourced information to make this possible.

The BBB Risk Index, with its multi-dimensional approach to evaluating scam risk, represents a major advance in our ability to take a data-driven approach to combating marketplace scams. It effectively distills the elements of risk we are able to glean from crowdsourced reporting into a single measure—one that is as powerful as it is simple to grasp and apply, both on a national scale and on a granular level. The Scam Tracker database allows us to parse the data to explore differences in risk borne by particular subsets of the population. Isolating data by cohort, geography, ...

In 2017, we witnessed a dramatic increase in scams being perpetrated online, thanks to a digital landscape that has become more and more complex with the introduction of new tools and platforms. ... This results in more dollars being lost by consumers and responsible businesses, and a potential downturn in online commercial growth.
income level, exposure, vulnerability, or loss can be helpful to those whose particular focus is devoted to helping that cohort. For example, if targeting messaging to millennials or seniors, it is important to know their particular vulnerabilities, as well as the medium and messaging most likely to reach them effectively.

In 2017, we witnessed a dramatic increase in scams being perpetrated online, thanks to a landscape that has become more and more complex with the introduction of new tools and platforms. Scammers take advantage of the ever-changing digital space, masquerading as reputable brands. This results in more dollars being lost by consumers and responsible businesses, and a potential downturn in online commercial growth. We are working to provide the tools to engage consumers and businesses in the fight against scams as they navigate the 21st century digital marketplace.

The insights provided by Scam Tracker are critical to providing the foundational data needed to tell the full story about the impact of scams. We are working with officials in business, law enforcement, and government to determine the best ways to stop scammers, and partnering with other stakeholders to help better allocate resources to tackle the problem and determine which prevention tactics are working, and which ones are not.

The 2016 Risk Report garnered a great deal of attention from the media, federal agencies, Congress and others, who recognized the importance of this new research. In October 2017, I was invited to testify at a hearing before the U.S. Senate Special Committee on Aging regarding robocalls and the impact of scams on older Americans. I was able to use Scam Tracker data to provide insights regarding automated calls targeted at seniors. Each new Scam Tracker research report provides new, relevant information that helps lawmakers make better decisions regarding scams and fraud.

In this year’s report, we’ve interviewed people who have been targeted by the top 10 riskiest types of scams and highlighted for you the things they wish they’d either known or done. This important research report is possible thanks to the brave men and women who chose to tell their stories.

The BBB Scam Tracker program exemplifies the BBB Institute’s work as the catalyst and spur for BBB innovation. This project is made possible thanks to the incredible work of BBBs across North America. Dedicated staff of each BBB review and compile the consumer reports that fuel the BBB Scam Tracker tool. Without their vision and dedication there would be no Scam Tracker and no BBB Scam Tracker Annual Risk Report. We’d also like to thank BBB CEO Warren King, president of the Better Business Bureau of Western Pennsylvania, who leads the Scam Tracker Task Force, and the entire Scam Tracker Task Force, whose leadership and service exemplify BBB. BBB Institute team members, Ayaz Minhas and Melissa Trumpower, have the pleasure of working with the Task Force to improve the tool and provide educational information and technical support to the entire BBB network. I thank them for their hard work.

The BBB Institute also wishes to thank the Council of Better Business Bureaus for its support and to recognize the contribution of its exceptional head of research, Rubens Pessanha, who somehow finds time to spearhead this research project every year, despite his many other projects.

Genie Barton,
President, Better Business Bureau Institute for Marketplace Trust
CONTENTS

2 FOREWORD
5 INTRODUCTION
6 SNAPSHOT OF 2017
8 BBB SCAM RISK INDEX
• Measuring the Overall Impact of Scams
• Risk Index Elements Defined
• Non-financial Costs of Scams
• Top 10 Most Risky Scams
11 VOICES OF SCAM TRACKER:
Victims Tell Their Stories
22 DEMOGRAPHICS
• Age
• Gender
• Geographic Area
26 SCAM DELIVERY AND PAYMENT METHODS
27 SPOTLIGHT ON MILITARY FAMILIES AND VETERANS
28 SPOTLIGHT ON STUDENTS
29 SPOTLIGHT ON IMPERSONATED ORGANIZATIONS
30 KNOW SCAMS
31 RESEARCH
32 LOOKING FORWARD
34 CONCLUSION
35 APPENDIX A
Glossary of Scam Type Definitions
37 APPENDIX B
Scam Data Table
38 APPENDIX C
Additional Stories from Victims
Marketplace scams represent a $50 billion drain on our economy, robbing consumers and legitimate businesses alike. Scams have a negative impact on one in four households and one in five individuals each year. Scammers masquerade as trusted brands, eroding consumer confidence in the marketplace. The continued fight against scams is critical to limiting the financial and emotional damage to victims and restoring consumer confidence in honest businesses so the marketplace can prosper.

By using technology to collect scam reports from consumers and businesses, and utilizing the power of our network of BBBs working in communities across the United States and Canada, BBB Scam Tracker maximizes our efforts to prevent scams and stop fraudsters. This data-driven approach utilizes limited resources to provide the greatest impact. BBB Scam Tracker collects timely reports submitted by scam victims and makes them available to the general public via an interactive website. The website enables anyone to search by keyword or pull reports by scam type, time period or geographic area. Reports are provided via an interactive “heat map” that enables consumers to zoom in on their own neighborhood or take in North America at a glance. This information informs our efforts to fight against scams. Data-sharing arrangements with the Federal Trade Commission and law enforcement ensure that this information is available for use in criminal and civil investigations. BBB Scam Tracker data are also made available to policymakers, consumer advocates, and educators.

Thank you to the consumers and business leaders who told their stories via BBB Scam Tracker. Thanks to their willingness to come forward, we are able to provide valuable insights into how to stop fraudsters and prevent others from becoming scam victims. The majority of those who report scams are motivated by the desire to make a difference by warning others, and the scams reported to BBB Scam Tracker do make a difference.

On behalf of the more than 100,000 citizen heroes who chose to speak out and report a scam since 2015, we are proud to present the 2017 BBB Scam Tracker Annual Risk Report. It is our belief that this report will advance marketplace trust by providing an in-depth picture of the scam landscape of 2017 and the methods used by fraudsters. The Annual Risk Report will support ongoing efforts to protect and inform the public and the business community.

In 2017, more than 47,000 scam reports were submitted to BBB Scam Tracker, an average of about one report every 11 minutes (Table 1), and an increase of 46 percent over 2016. These reports were received from both businesses and individuals in North America, representing a cross-section of the population. Reports were classified into 30 scam types (Appendix A), including an “other” category representing 3.8 percent of all reports. Data collected included a description of the scam, the dollar value of any loss, and information about the method of contact and means of payment. The age, gender and postal code of the victim or target were also collected along with military (active duty, veteran or spouse) and/or student status. See Appendix B for more detailed data by scam type.

New, creative scams pop up every year, and 2017 was no different. Telephone was once again the top means of contact. The ever-increasing numbers and new types of robocalls spurred the concerted action of industry and consumer stakeholders, as well as inquiries and initiatives from Congress, federal and state regulators and law enforcement agencies at every level. The Federal Communications Commission estimated that 2.4 billion robocalls were made each month in 2016; approximately 6 percent of the scams (primarily tax collection, travel/vacation and credit card) reported to BBB Scam Tracker in 2017 had “robocall” in the narrative. New call blocking technologies are available. The best advice is not to answer a phone call from a number you don’t know.

Scammers continued to use social media to engage with victims, utilizing Facebook, SnapChat and other online platforms to connect with victims and impersonate their friends and family. Email also remains a common method of contact, with scammers spoofing legitimate businesses to take advantage of victims. Those looking to plan their dream
<table>
<thead>
<tr>
<th>Table 1: Snapshot of 2016 vs. 2017</th>
<th>2016</th>
<th>2017</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of BBB Scam Tracker Reports</td>
<td>32,781</td>
<td>47,827</td>
<td>46%</td>
</tr>
<tr>
<td>% Susceptibility (i.e., % of reports that included $ Loss)</td>
<td>18.8%</td>
<td>15.8%</td>
<td>-16%</td>
</tr>
<tr>
<td>Median Dollar Loss</td>
<td>$274</td>
<td>$228</td>
<td>-17%</td>
</tr>
<tr>
<td>Top Means of Contact</td>
<td>Phone</td>
<td>Phone</td>
<td>N/A</td>
</tr>
<tr>
<td>Top Method of Payment</td>
<td>Credit Card</td>
<td>Credit Card</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Vacations were targeted by scammers, with imposter property owners offering attractive alternatives for booked venues, and then sending victims to fake payment sites. Victims realized too late that the venue either didn’t exist or belonged to someone else.

The good news, though, is that overall, the susceptibility to scams reported to BBB Scam Tracker decreased from 18.8 percent in 2016 to 15.8 percent in 2017. And the median dollar loss also decreased to $228, a 17 percent decrease from 2016.

More good news – BBB observed a decrease of more than 60 percent in the number of scam reports related to tax collection in 2017. This was likely related to the arrest of the alleged ringleader of the IRS scam.5 On the other hand, 2017 was the year of the “Can You Hear Me?” calls, and we received more than 10,000 reports with “Can You Hear Me” narratives.6 However, the susceptibility (i.e., percent of people who reported monetary loss) of these calls appears to be zero (i.e., we could not identify a single credible report with a genuine monetary loss). Thus, we do not have any credible evidence in BBB Scam Tracker that the “Can You Hear Me” issue should be categorized as a scam. Also, after controlling for the “Can You Hear Me?” narratives, we saw significant increases in reports of phishing (439 percent); travel/vacation (256 percent); and healthcare/Medicaid/Medicare scams (136 percent).

---

2 All dollar values in this report have been converted to USD.
4 Because Scam Tracker does not currently ask consumers specifically whether a telephone call was initiated using an autodialer, this statistic may undercount robocalls.
6 To read more about “Can You Hear Me,” visit https://www.snopes.com/can-you-hear-me-scam/.
Measuring the Overall Impact of Scams

Last year’s BBB Scam Tracker Annual Risk Report introduced the BBB Risk Index to more effectively measure the overall impact of scams. Previous attempts to compare scam types by relative risk had generally consisted of simple rankings by frequency of exposure. This volume-based approach failed to acknowledge the multifaceted nature of scam risk. The BBB Risk Index posits that the risk posed to a given population by a particular scam type can best be understood by considering three dimensions: exposure, susceptibility, and monetary loss. By combining all three, we are able to gain a far more meaningful measure of the relative risk of a given scam type.

It is important to acknowledge that no measure of risk is without limitations. As the Index is calculated using data collected through BBB Scam Tracker, we are limited by the very nature of self-reporting as an imperfect measure of the extent of the problem. Because of the embarrassment associated with being a scam victim, it is likely that there is significant under-reporting of scams. Moreover, while BBB reviews reports to determine if they describe what a reasonable person would believe to be a scam, these reviews do not validate consumer allegations. The Index does not factor in the emotional and psychological harm scams can inflict, nor does it provide a measure of the loss to legitimate businesses by the misuse of trusted business names and services to perpetrate fraud. Finally, even among those who are able to avoid a monetary loss, exposure to scam attempts can be an unsettling nuisance, contributing to lost time and diminished trust in the integrity of the marketplace, none of which can be captured by the factors used in the Index.

The information provided by use of the Risk Index and the various charts and tables in this report can be drivers for focusing educational and investigative efforts where they are likely to have the greatest effect. These data also can be used to understand how risk varies by geographic region and by particular subgroups of the population, such as military personnel and students, and by age.

To better understand the rationale for the Index, consider the variable nature of the scam landscape. On one end of the spectrum, a fraudster may employ a “wide net” approach, using mass email or robocalls to reach perhaps hundreds of thousands of individuals to find those few who would succumb to the ploy. These scams reach a wide swath of the population, but the susceptibility of those exposed is likely to be relatively low. At the other end of the spectrum is the far more intensive “high-touch” approach, as is commonly seen with romance and investment scams. These scams reach fewer individuals, but those exposed are often more likely to be successfully conned.

Monetary loss is a final critical element. A con that separates mere pennies from its victims may do tremendous overall harm if it impacts a large portion of the population, while a scheme with relatively few victims may be of great concern if median losses are extremely high. The Index captures these real-world elements by representing the intersection of exposure, susceptibility and monetary loss.

Non-financial Costs of Scams

Marketplace scams represent a $50 billion scourge on our economy that impacts one in four households and one in five individuals each year.7 But what is less known is the overall human impact of fraud on people. According to research by the FINRA Foundation, a longtime partner of the BBB Institute, the non-financial costs can include stress, depression, frustration, anger, sleep deprivation, health issues, lost time and other psychological consequences.
While each of these examples may also entail additional financial losses, the overall impact on health and well-being has not been extensively researched at this time and is not currently included in our risk index.8

**Top 10 Most Risky Scams**

The table on page 10 reflects the top 10 most risky scam types based on all reports submitted to BBB Scam Tracker in 2017 (United States and Canada).9 Online purchases took over the top spot as the most risky scams. With people buying more things online than in stores, the bump is not surprising, and helping people be safe online is an important topic for programmatic consideration.10

The majority of online purchase scams occur when a payment is made online in exchange for a good or service, but nothing is delivered. These scams can encompass a number of different types of purchases. The most common online purchase scams in 2017 were related to pets, clothing, cosmetics, electronics, and automobiles (Table 3). The offer of free trials was a common tactic for these online purchases; 67 percent of scams involving cosmetics and 60 percent involving nutrition products mentioned a free trial opportunity.

In order to succeed, scammers often rely on the following tactics:

- The promise of getting a great deal, which is often too good to be true;
- Pressure to respond immediately, not letting people second-guess the situation (e.g., “they said the sale offer was time sensitive and the price couldn’t be guaranteed if I called back 20 minutes later”);
- Some sort of power pressure, including intimidation (e.g., “You are under federal investigation”; “You will be arrested within one hour unless you call this number”); and
- Isolation, which aims to force a decision without others’ opinions.

The risk of investment scams also increased significantly in 2017, as compared to 2016. This was primarily due to an increase in median monetary lost, with exposure and susceptibility not significantly deviating from 2016 to 2017. Another notable change from 2016 is the drop in reported home improvement scams (down from the No. 1 spot to No. 6). These scams ranked as the No. 1 most risky in 2016 due to high susceptibility (targets are less likely to recognize and avoid the scam).

Surprisingly, the drop occurred in a year marked by several weather-related disasters, including Hurricanes Irma and Harvey. Contrary to previous years, we saw a significant amount of information from the media and consumer protection groups – many of them coming from BBB – around home improvement scams following disasters.

---


10Even after controlling for the impact of “Can You Hear Me” calls, the top 10 risky scams remained the same.

11http://fortune.com/2016/06/08/online-shopping-increases/.

---

**Risk Index Elements Defined**

**Exposure** is a measure of the prevalence of a scam type, calculated as the percentage of all scams reported, represented by that scam type. This calculation includes scam reports by those who suffered monetary losses and by those who were exposed to scams, but avoided losses. A relatively high exposure measure indicates a greater likelihood of being targeted by a particular scam type, while a relatively low exposure measure indicates that a scam type is less common.

**Susceptibility** is a measure of the likelihood of losing money when exposed to a scam type, calculated as the percentage of all reports of the scam type that involved a monetary loss. A low susceptibility rate indicates a high probability that the scam type will be recognized and avoided, while a high susceptibility rate indicates that targets are less likely to recognize and avoid the scam.

**Monetary Loss** is calculated as the median dollar amount of losses reported for a particular scam type, excluding reports where no loss occurred.
Among the top 10 risky scams in 2017, two new scams joined the list (travel/vacation and government grant) and two left the list (romance and sweepstakes/lottery/prize). The top destinations included in the narratives of the travel/vacation scams in 2017 were:

1) Orlando/Florida (276);  
2) Disney (214);  
3) Mexico/Cancun (70); and  
4) Bahamas (62).

It is also important to note that even though fake check/money order scams dropped from the second spot in 2016 to the fifth in 2017, the usage of fake checks is a common tactic used by scammers in other types of scams, primarily employment and sweepstakes/lottery/prize. It is important to convey the message to the public at large that a check can bounce even after it “clears” and your bank allows you to withdraw cash from that deposit. Unfortunately the term “clear” can be used prematurely by bank employees.\(^1\)

---

**Table 2: Top 10 Riskiest Scams of 2017**

<table>
<thead>
<tr>
<th>#</th>
<th>Scam Type</th>
<th>BBB Scam Risk Index</th>
<th>% Exposure</th>
<th>% Susceptibility</th>
<th>Median $ Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (4)↑</td>
<td>Online Purchase</td>
<td>30.9 (23.0)↑</td>
<td>9.7% (8.4%)↑</td>
<td>72.5% (74.1%)↓</td>
<td>$100 ($101)↓</td>
</tr>
<tr>
<td>2 (6)↑</td>
<td>Investment</td>
<td>25.6 (19.8)↑</td>
<td>0.5% (0.6%)↓</td>
<td>50.8% (51.0%)↓</td>
<td>$2,310 ($1,800)↑</td>
</tr>
<tr>
<td>3 (3)↓</td>
<td>Employment</td>
<td>24.6 (25.8)↓</td>
<td>5.1% (6.3%)↓</td>
<td>13.8% (16.7%)↓</td>
<td>$800 ($671)↑</td>
</tr>
<tr>
<td>4 (5)↑</td>
<td>Advance Fee Loan</td>
<td>22.7 (22.4)↑</td>
<td>2.2% (3.3%)↓</td>
<td>38.9% (36.4%)↑</td>
<td>$600 ($510)↑</td>
</tr>
<tr>
<td>5 (2)↓</td>
<td>Fake Check/Money Order</td>
<td>21.3 (25.9)↓</td>
<td>2.3% (3.1%)↓</td>
<td>14.2% (15.8%)↓</td>
<td>$1,488 ($1,471)↑</td>
</tr>
<tr>
<td>6 (1)↓</td>
<td>Home Improvement</td>
<td>18.9 (26.8)↓</td>
<td>0.8% (1.0%)↓</td>
<td>44.9% (53.4%)↓</td>
<td>$1,255 ($1,400)↓</td>
</tr>
<tr>
<td>7 (8)↑</td>
<td>Tech Support</td>
<td>16.5 (12.0)↑</td>
<td>4.8% (4.8%)↑</td>
<td>26.4% (22.9%)↑</td>
<td>$300 ($299)↑</td>
</tr>
<tr>
<td>8 (12)↑</td>
<td>Travel/Vacation</td>
<td>10.2 (10.8)↓</td>
<td>5.4% (0.9%)↑</td>
<td>3.7% (38.0%)↓</td>
<td>$1,184 ($847)↑</td>
</tr>
<tr>
<td>9 (9)</td>
<td>Family/Friend Emergency</td>
<td>9.6 (11.2)↓</td>
<td>0.7% (0.8%)↓</td>
<td>10.3% (18.8%)↓</td>
<td>$3,000 ($2,174)↑</td>
</tr>
<tr>
<td>10 (11)↑</td>
<td>Government Grant</td>
<td>9.4 (11.1)↓</td>
<td>4.1% (4.8%)↓</td>
<td>10.3% (9.6%)↑</td>
<td>$500 ($650)↓</td>
</tr>
</tbody>
</table>

**Table 3: Top Product Categories of Online Purchase Scams**

<table>
<thead>
<tr>
<th>Product</th>
<th>Details</th>
<th>% Exposure</th>
<th>% Susceptibility</th>
<th>Median $ Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pets</td>
<td>Puppies, kittens, birds, exotic animals</td>
<td>22%</td>
<td>58%</td>
<td>$600</td>
</tr>
<tr>
<td>Clothing</td>
<td>Clothing, jerseys, jewelry, shoes</td>
<td>22%</td>
<td>85%</td>
<td>$65</td>
</tr>
<tr>
<td>Cosmetics</td>
<td>Skin creams, lotions, makeup, perfumes, soaps</td>
<td>17%</td>
<td>84%</td>
<td>$162</td>
</tr>
<tr>
<td>Electronics</td>
<td>Cell phones, laptops, cases, headphones</td>
<td>9%</td>
<td>67%</td>
<td>$97</td>
</tr>
<tr>
<td>Automobile</td>
<td>Cars, car parts, motorcycles</td>
<td>8%</td>
<td>42%</td>
<td>$1,500</td>
</tr>
<tr>
<td>Nutrition</td>
<td>Supplements/extracts for health, weight loss</td>
<td>5%</td>
<td>86%</td>
<td>$148</td>
</tr>
<tr>
<td>Tickets</td>
<td>Concert/event tickets</td>
<td>3%</td>
<td>85%</td>
<td>$170</td>
</tr>
<tr>
<td>Hobby</td>
<td>Guns, bicycles, toys, collectibles</td>
<td>3%</td>
<td>86%</td>
<td>$88</td>
</tr>
<tr>
<td>Furniture</td>
<td>Lamps, rugs, clocks, blankets, candles</td>
<td>2%</td>
<td>77%</td>
<td>$85</td>
</tr>
</tbody>
</table>

VOICES OF SCAM TRACKER: VICTIMS TELL THEIR STORIES

The findings provided in this report are possible thanks to the real people targeted by scams, who chose to report them. The data outlined within these pages provide critical insights about the trends in scams and the vulnerabilities of particular populations. But it’s the personal stories of scam victims that bring home the human dimension of scams. The BBB Scam Tracker database provides consumers’ stories in their own words. These stories provide valuable insights into the psychology of scammers and their victims.

In preparing the 2017 Risk Report, we reached out to a number of the victims who were brave enough to share their stories. Through our conversations with these individuals, we were able to learn more about the tactics scammers use and what psychological effect these tactics had on the victims. Sometimes, warning bells went off and the scammers were unsuccessful. Other times, the scammers succeeded. But in either case, these stories reveal a great deal about the manipulative tactics scammers use, from promises of financial gain to intimidation. We thank the people whose stories are recounted here. Their hope, as is ours, is that by bringing to light the tactics scammers use, we can warn others and help consumers spot the signs of a scam.

*At their request, some of the names of the victims have been changed.*
BUYERS BEWARE: SCAMMERS WILL SPOOF LEGITIMATE COMPANIES

Jim was searching for a new truck he could use both at home and for work. He spent months searching for a good deal online and at dealerships, and finally came across a listing on Craigslist that would fit his needs and be within budget. He replied to the ad and began an email conversation with a kind widow named Arlena Berston. She said she was selling her late husband’s truck, and was offering a good deal because “seeing that truck every day reminded her of her husband and her children’s father.” Jim and Arlena took the conversation from email to phone as they discussed the details of the purchase.

“I really felt for their family,” Jim recalls. “We joked back and forth and I developed a relationship with these folks.” Arlena suggested making the sale through eBay’s Vehicle Protection Program, Jim recalls, “so that we were both safe with our contract of sale and delivery.” That seemed like a great idea to Jim, who passed along his contact information to Arlena so she could set up the transaction with an eBay agent. An agent named Frankie Hayes reached out. He sent Jim a bill of sale and purchase order number on eBay letterhead. Frankie also sent Jim links to eBay’s privacy policies and its Vehicle Protection Program information. Everything would be handled by eBay directly. At the same time Jim was negotiating the terms and conditions of the sale, he was still keeping in regular contact with Arlena about travel logistics. Should he fly to Nebraska to meet her, or would the car be shipped to him? Who would pay for those costs? Jim tried to remain flexible, considering Arlena’s sensitive family situation.

They agreed to split the costs for Jim’s plane ticket from California to Nebraska, and Jim followed Frankie’s instructions on how to process the payment; he sent $1,500 for the car, plus a $60 processing fee in the form of a MoneyGram to Frankie Hayes via the eBay Motor Agency in Mississippi. He was also told to declare that the MoneyGram was for a relative or friend so the “transfer commission” would be less. The next day, Frankie confirmed he had received the funds and sent Jim a receipt.

Jim didn’t hear from Arlena for a few days, but it was Thanksgiving. While he was anxious to get his new truck, he didn’t want to interrupt such an important family holiday. He continued to borrow his wife’s car for work, but they needed the truck to come soon. Then, out of the blue, an email arrived with a shipping notification for the truck. The shipper said he’d contact Jim when he was six hours away to schedule the drop off. That was the last time Jim heard from Arlena, Frankie, or the shipper, and his attempts to get his money back from eBay or by working with the local police yielded no success.

Jim reported his story via BBB Scam Tracker to help others. “Everything about what [happened] seemed 100 percent legitimate,” he says. “[I] figured I was going through so much—maybe I can let someone else know so they don’t go through it and end up in the same situation.”

What Jim wants you to know:

• Check website links and the sender’s email address. A scammer may try to spoof some content, but in this case the emails came from checkout@motor-program.com. While not initially alarming, in hindsight, he notes that they should have had an @ebay.com email domain.
• Consider making large purchases (such as a car) in person. Physically examine what you’re buying before you pay for it.

Additional tips from the BBB:

• An unreasonably low price should be a warning sign. Proceed with caution, even if there’s a realistic-sounding story behind the price point.
• Pay for purchases through a secure payment method like a credit card. If a seller asks you to wire money and you’ve never met the person or seen the product, you should decline.
• Scammers copy links, images, and text from legitimate companies. When in doubt, go to the purchasing site separately, log into your account, and make sure the purchase information is accurate.

Data snapshot:

• Primary means of contact with monetary loss: website
• Primary payment method: credit card
#2: INVESTMENT SCAMS

HIGH-VALUE INVESTMENTS REQUIRE DUE DILIGENCE

Pat received an email inviting her to participate in a lucrative investment opportunity. Curious, she called the number and spoke with Patrick Collins from Starling Capital Bank.

“He was so nice and sweet,” Pat recalls. “He said he would help me all the way.”

Patrick explained that his company gives his investors huge returns on their money, allowing them to track the progress through the company’s online platform. Pat didn’t know much about investing, but the website looked legitimate and Patrick sounded knowledgeable, so she put $300 in an investment account with the bank to see what happened.

Within days, she logged on to the Starling Capital Bank website and saw huge growth—she now had $800! She withdrew the funds just to see what would happen, and received it back in her account. Happy with her success, Pat decided to deposit another $500. Patrick called and encouraged Pat to put more money in; he said she’d see even greater success if she put in a larger amount. So she invested $1,000 more. A few days later, it had grown to $33,000. “It happened so quickly, and I was totally excited!” she remembers.

Patrick called to congratulate Pat. He said she’d be amazed what would happen if she put in an additional $5,000. She didn’t have that kind of money to spare, so she took out a personal loan. Excited and nervous, she watched her investment double as Patrick had promised.

Pat felt on top of the world, and was just about to tell her friends about this amazing opportunity when the unthinkable happened. She checked her account and her balance was $75. She was furious. How did all of this money disappear? She called Patrick, who explained that it’s not uncommon for foreign investments to tank—that it was part of the risk she’d taken as an investor. He encouraged her to try again and put in a few more thousand.

Pat argued with him: “You took my $6,000 and I thought it was a good thing!”

When she got nowhere with Patrick, Pat reached out to Starling Capital Bank. Their representatives said that all transactions are handled by the broker, which in her case was Patrick. That’s when she decided to investigate the legitimacy of the business and Patrick as her broker—and when she realized it was a scam.

“He didn’t help me, he helped himself. I lost everything.” For months, she didn’t tell anyone about the experience. She still had to pay off the loan for the money she invested. “I was so ashamed, I didn’t want anyone to know.”

But after opening up to a few close friends and family members, she decided to share her story on BBB Scam Tracker. “After all that happened, who knows, [maybe now] someone else will think before they invest.”

What Pat wants you to know:

• Verify the company or investment broker is licensed or registered before you give them any money. In the United States, check FINRA.org; in Canada, contact the Canadian Securities Administrators (CSA).

Additional tips from the BBB:

• Be wary of deals that sound too good to be true or deals that offer low to no risk with high return.

• Avoid high-pressure sales tactics.

• Even if you’re dealing with somebody who seems friendly and nice, do your homework.

• The “investor” may look polished and seem professional, but take time to think about your investments. Go with your gut. If something feels off, walk away.

Data snapshot:

• Primary means of contact with monetary loss: phone

• Primary payment method: wire transfer
BEWARE OF DREAM WORK-FROM-HOME JOB OFFERS

Juanetta needed a new job that would fit her busy lifestyle, so she posted her resume on a few employment websites. She was elated when she received a text from a woman named Sandra Pat, who had found Juanetta’s resume on Ziprecruiter.com. Sandra told her about a data analyst/administrative assistant position that sounded like a great fit—the pay was $25.75 per hour and it was a work-from-home opportunity. Sandra passed along the contact information for Angeline Felicia, her company’s interview manager, who set up a time to talk via Google Hangouts.

“She took me through a series of questions,” Juanetta recalls. But the interviewer dropped off before she could ask more about the opportunity. The next morning, Juanetta got a text—she’d gotten the job! She was then introduced to her new supervisor, Julie Iwashita.

“Julie explained my duties, sent me an offer letter and NDA to sign, and informed me I would be given a training task every day for a week to prepare for the job,” says Juanetta. “She also mentioned that the company left no stone unturned when it came to providing employees with state-of-the-art equipment for the job, so a check would be sent to cover the costs of equipment for a home office.”

The check arrived a few days later via UPS, and Juanetta was told to deposit it via ATM into her bank account. When she mentioned she could go to her local branch to deposit the check, she was sternly reminded to make the deposit via the ATM. Juanetta thought her new employer’s reaction was strange. What did it matter how she deposited the check?

“I was going to deposit it in the bank anyway, but because it was so cold outside, the line was long inside the bank.”

Juanetta deposited the check in the ATM machine outside. When the check cleared her bank a few days later, she was told to go to her bank, withdraw $4,700, and deposit it into an account at Bank of America. This would enable the local vendor to purchase her home office equipment.

“This set off red flags,” she recalls. “If I wasn’t going to purchase the items, why not just send the money to the vendor yourself and send me the equipment?”

She asked if she could do an electronic transfer instead. Her employer agreed, but there were a series of incorrect accounts given to her with mismatching account information. The bank called to tell her they couldn’t do the transaction.

“Something still didn’t feel right to me.”

Her skepticism had led her to take a photo of the check before she deposited it, which turned out to be the proof she needed to get out of the situation; when she called the bank in Texas where the check was drawn, they told her it was counterfeit. She canceled the electronic transfer, which had not yet been processed.

“I was totally embarrassed,” she says. “When I told my bank, they said they were so sorry it happened to me and told me not to be embarrassed. The scammers are professionals, and lots of people fall prey.”

Juanetta decided to report the incident via Scam Tracker, where she found another person who had been targeted by the same people.

“If this helps someone, it was worth it.”

Juanetta’s lessons for others:

• Listen to your gut instincts. “There were a few times when something felt off, but I let it go.”
• If you’re looking for at-home work opportunities, search for the company and opportunity online. “I searched for scams similar to mine and found one on Scam Tracker in my area that used the same first names and sounded almost exactly alike. There are probably others out there too scared to share what happened to all of us.”
• Verify the company’s contact information. If they aren’t willing to provide a phone number and address you can verify is real, it may be a scam.

Additional tips from the BBB:

• A reputable employer will give you the equipment you need; they won’t give you a check to deposit and subsequently wire elsewhere in order to purchase your needed supplies.
• Don’t be embarrassed; this can happen to anyone, and it does.

Data snapshot:

• Primary means of contact with monetary loss: email
• Primary payment method: other
#4: ADVANCE FEE LOAN SCAMS

**LEGITIMATE LOANS SHOULD NOT REQUIRE ADVANCE PAYMENT**

Eva needed a little extra money, so she went online to search for a credible place to get a small personal loan. She found a company that appeared legitimate, provided her bank account information, and signed the necessary paperwork via email. The process seemed easy and professional. All seemed fine until the company called her later that evening and asked her to go to Walmart to buy two $400 gift cards. Once she sent them the cards, the company would release the funds.

“That’s when I knew it was a scam,” recalls Eva. “It makes no sense that they would want me to go to Walmart to buy gift cards for a loan.”

Eva called her bank, and it told her the funds had been transferred to her account via a mobile device, but were not released. The bank confirmed it was a scam.

“I ended up with restrictions on my bank account because I gave them my banking information.”

Eva says having her accounts frozen while the bank prevented further fraud was more frustrating than the loan experience itself. When she told a friend about the situation, the friend told her she wished Eva had said something sooner, because she would have told her not to trust the company. Eva reported the incident via BBB Scam Tracker.

“I didn’t want anyone else to go through this.”

**Additional tips from the BBB:**

- Any up-front fee you need to pay to get a loan is a cue to walk away. A real lender will post fees prominently and collect them from the money they are lending to you, not as a condition for you receiving funds.
- Fees should not be paid via gift cards or wire transfers.
- Lenders and loan brokers must register where they do business. Check with your state or provincial/territorial government to verify loan brokers’ registration.

**Data snapshot:**

- Primary means of contact with monetary loss: phone
- Primary payment method: prepaid card

---

What Eva wants you to know:

- Verify the loan company’s information. Make sure it has valid contact information on its website.
- If they are asking for your information and password to log into your bank account, it’s a bad place to get a loan.
FREE? UNEXPECTED PAYDAY? IT’S LIKELY A SCAM.

Getting an unexpected check in the mail is something we’d all like to experience. It happened to Rachel, who found a USPS Priority Mail envelope in her mailbox containing a $2,250 check. The check was from a company called Market Force and included a letter congratulating her for being accepted into its secret shopper program. “I never signed up to be a secret shopper, but to the quick eye, it looked real,” she recalls.

The letter said she’d be evaluating Wal-Mart stores in her area, and as part of the shopping spree she should purchase an item costing less than $50, and make two wire transfers for $900 each.

Rachel had received multiple emails and text messages from the company. “[It] made me feel uneasy that they had all of my contact information—my phone number, my email address, [and] my home address.”

While she would have liked the extra money, she suspected the check was fake and did not deposit it, despite receiving frequent messages from the company asking why she had not yet cashed the check. Rachel had been subjected to a lot of different scams, and her father fell victim to a fake check scam, so she knew better than to deposit the check in her account. Her goal in reporting the scam was to protect those who are vulnerable to these kinds of scams, including the elderly and young students. If the check is fake, the bank will find out eventually and withdraw the funds.

What Rachel wants you to know:

• Question unsolicited funds: “No one just sends you a big check for no reason.”
• Verify the business’ contact information. The email address given to her was marketforce@offensivelytolerant.com (not exactly an accurate or professional domain).
• Remember, just because the check “clears” the bank does not mean it’s not fraudulent. It may takes weeks for the bank to realize it is a fake check.

Additional tips from the BBB:

• Be immediately suspicious of overpayments. If someone gives you a check and wants a cut of it back, it may be a scam.
• Never send money to people you do not know, especially if they ask for money via wire transfer or prepaid debit or gift card.

Data snapshot:

• Primary means of contact with monetary loss: email
• Primary payment method: check
#6: HOME IMPROVEMENT SCAMS

ALWAYS RESEARCH A COMPANY BEFORE DOING BUSINESS, EVEN IF YOU KNOW THE CONTRACTOR PERSONALLY

Lindsey was doing some work on her back yard, and thought a deck would be the perfect addition. While searching for contractors, her boyfriend suggested a man named Howard Norman of Jarhead Landscaping—they were softball buddies and he knew Howard was an ex-Marine. They’d even had dinner with Howard and his wife.

“I trusted him because he had been in my home and had even offered to babysit,” Lindsey recalls.

They met one day at The Home Depot to discuss building supplies, and Howard said some of the supplies would need to be specially ordered. He said he had a business account with The Home Depot, so it made sense for him to buy the materials and then pass along the savings. He said he had a friend at the store who would make sure they got a good deal on some quality materials. Lindsey gave him $5,000 and waited for the supplies to arrive at her home. They never showed. She texted back and forth with Howard, because she wanted it all in writing. Eventually, she gave up on ever seeing the materials and demanded a refund.

“I have proof—he sent me more than 20 text messages saying the check was on its way to repay me the money that he owes me, and each time he had a lie or an excuse,” she recalls.

Lindsey threatened to call the police, and Howard refunded her $1,200, saying that’s all he had. Frustrated and angry, she went online to leave him a poor review. That’s when she saw the unthinkable. Howard had posed as Lindsey on a reviewing site and had written a glowing review of his own work.

“What he did is horrible. He’s a true con artist.”

What Lindsey wants you to know:

• “Get references”—especially from people who have had projects completed by the contractor, not just from those who know the contractor personally.
• Verify the contractor is licensed and insured. “I knew better, but I thought I knew him well.”

Additional tips from the BBB:

• Beware of high upfront payments, cash-only deals, high-pressure sales tactics, “handshake” deals without a contract, and on-site inspections.

Data snapshot:

• Primary means of contact with monetary loss: in-person
• Primary payment method: check

not only taken money from 11 homeowners, but had perpetrated scams in three other states.

“I have no idea how many people were affected,” says Lindsey. “Some people are just afraid to speak out because that’ll make him mad and they may never get their money back.”

While Lindsey felt vindicated that she had reported the scammer and banded together a great support system of people online who had experienced the same loss, it strained her relationship with her boyfriend.

“It caused so much collateral damage. I didn’t blame my boyfriend at all [for introducing us], but there was so much going on,” she says.

Lindsey had other projects she wanted to complete around her home, but this experience soured her desire to make her yard a beautiful place to relax after a long day of work.

“What he did is horrible. He’s a true con artist.”
#7: TECH SUPPORT SCAMS

LOUD, FRIGHTENING COMPUTER SUPPORT WARNINGS: DON’T ENGAGE

Terre was spending a quiet evening playing games on her computer when a screen popped up with an extremely loud alarm sound. The screen said, “WARNING! You have been infected with a virus, do not leave this page. Do not turn your computer off, or you will not be able to use it again.” A loud voice told her to call the phone number on the screen immediately.

“My mind was going 3,000 miles per hour,” Terre said. “My grandson gave me that computer for Mother’s Day. It was important that I be able to use that computer again.”

She called the phone number, and a representative told her the computer was infected, but it could be fixed for $169. She told him she had McAfee security software. The representative told her his company was not affiliated, but it could tell that her copy of McAfee was outdated. The rep stayed with her on the phone for hours as she watched the work being done on her computer, and nervously waited to see if it would be functional again. When the rep asked for her credit card, she agreed. She thought about how her sister’s computer had had a virus a few weeks back that ultimately couldn’t be fixed and she had to buy a new one. Paying $169 was definitely better than buying a new computer. By 3:30 a.m., the rep said he had finished fixing more than 6,000 corrupted files and wanted to know if Terre wanted to extend coverage for a few years. Tired and drained, she agreed, bringing the total to $515.

A few days later she called McAfee to ask why its security software did not catch the virus. The representative told her she’d been scammed. She called the scammers back and was promised a refund within a week, but it never arrived. The bank refused to refund her money because she had given permission for the service. Terre reported the incident via BBB Scam Tracker, but says she almost didn’t because she felt foolish.

“If this is how I felt, others will feel the same if it happens to them.”

What Terre wants you to know:
• Slow down and trust your instincts. “Deep inside I knew this was wrong. It’s easy to get caught up in the stress of the moment, but step back, look at it again, and heed your instincts.”

Don’t fall for their scare tactics. “They scare you so much that you’re just about willing to do anything to fix it!”

• Hang up and reach out to someone for advice. Do not let them tie up your phone line for hours.
• Just turn off the computer. Step away, calm down, and then reboot it—even if the screen says not to.

Additional tips from the BBB:
• Never give control of your computer to a third party unless you know they are a representative of a legitimate computer support team you contacted.
• Legitimate tech support companies do not call out of the blue.
• If you are the victim of a tech support scam, take your computer to a trusted local business and have it checked out, and change the passwords you use to access important online accounts, including online banking.

Data snapshot:
• Primary means of contact with monetary loss: phone
• Primary payment method: credit card
#8: TRAVEL/VACATION SCAMS

SCAMMERS CAN BE FOLKSY AND CHARMING: DON’T BELIEVE EVERYTHING YOU HEAR

Edwin is an experienced IT consultant who considers himself someone who can spot a poorly executed scam quickly. So when he was approached by a Midwestern farmer named Bob McMahon with a seemingly authentic Midwest accent who was interested in purchasing his timeshare, he stopped to listen. The man said he’d been turned off by a pushy salesman in Mexico, but was still interested in purchasing Edwin’s Mexican timeshare if they could go through his friend’s title company.

“They were very convincing and their acting was superb,” Edwin recalls. “The guy sounded like a good ol’ boy from the Midwest, and said he was buying it for his wife’s birthday. The pricing was right and it sounded so legitimate.”

Edwin spoke with both men, who had elaborate personal stories that seemed too detailed not to be true. But when he was told there would be two fees to complete the sale (he’d pay the small fee of $2,750; they’d pay the larger fee), he began to suspect something was amiss. When he suggested they take the fee out of escrow, they pushed back and said Mexico would not allow that.

Edwin then set out to dig deeper to determine if the men were scammers:
- He checked on the authenticity of the title company, but was unable to verify the title company’s registration in the state of Missouri.
- Upon further research on whois.icann.org, he found that the website was set up and owned by Mexican interests.
- The company’s address seemed right on first glance, but the suite number was missing. He realized that though it’s a real building, they didn’t really have an office there.
- The phone number was not traceable (he Googled the number, which was connected to an international number, indicating it was being bounced).

Edwin reported the incident via BBB Scam Tracker because, despite his background, he was surprised by how real the scammers seemed.

What Edwin wants you to know:
- Take the time to investigate every detail. It’s easy to put up a professional-looking website these days, but it’s much more difficult to register a domain. If you look close enough, you’ll find the red flags.
- Never share your banking information; if you need to pay, use a credit card.

Additional tips from the BBB:
- Don’t be fooled by a good “back story.” Scammers who target individuals in high-value scams can be very skilled at making up plausible and charming fake identities.
- If you are told to use a particular title company or escrow agent, beware. This may signal that this is an elaborate scam.

Data snapshot:
- Primary means of contact with monetary loss: phone
- Primary payment method: credit card
SCAMMERS PREY ON THOSE WANTING TO HELP THOSE THEY LOVE

Charles and his wife received a phone call every parent and grandparent dreads—their grandson had been in a car wreck. The caller, who said he was calling from an organization called Legal Aid, told Charles and his wife that their grandson was okay, but that he’d been arrested for DUI and was in custody for hitting a woman who was eight months pregnant. The callers said their grandson needed $6,500 for bail. Charles’ wife was distraught.

Charles took the phone from his wife, and the callers then put his grandson on the phone.

“It did sound like him,” he recalls.

But the man on the other end of the phone was unable to tell Charles his full name. Charles, who had read about the “grandparent scam,” hung up the phone. They immediately called their daughter and confirmed that the grandson was at home and safe.

“If they had done their homework, they may have gotten me,” Charles says. But, he added, the fact that his own grandson couldn’t remember his own name made it clear it was a scam.

What Charles wants you to know:

• If possible, call the friend/relative in question, or somebody who is close to them, as soon as possible to confirm they’re in trouble.

Additional tips from the BBB:

• Resist the urge to act immediately, no matter how dramatic the story is. Check out the story with other family and friends, but call directly. Don’t call the phone number provided by the caller or Caller ID. Ask questions that would be hard for an impostor to answer correctly.

Data snapshot:

• Primary mean of contact with monetary loss: phone
• Primary payment method: prepaid card

If possible, call the friend/relative in question, or somebody who is close to them, as soon as possible to confirm they’re in trouble.

• Know what your family members are sharing online. You may not have control over your family’s social media accounts, but familiarize yourself with what they are sharing online.
GOVERNMENT GRANTS SHOULDN’T REQUIRE UP-FRONT FEES OR TAXES

College is expensive, so when somebody calls to say you qualify for a $9,200 government grant, you listen. Corey was thrilled at the prospect of getting a little extra help. He was given an activation number and a phone number for a representative who would help him through the process. He even received an email with the grant check, which looked authentic.

“The first thing they made me do was buy $200 in iTunes cards so I could activate the process,” he recalls. “Then they told me I had to pay $500 for a state tax since I live in Georgia and the bank was located in New York.”

Even then, the scammers weren’t finished asking for upfront payments from Corey. They told him the last step was to pay $1,200 for “clearance.”

“I only had $600 left, so I gave it to them,” he says. In order to finish paying off the remainder of the “clearance fee,” he was asked to buy more iTunes gift cards. The callers promised he’d receive all of these fees back, along with the $9,200 grant. Corey asked his mother for advice, who apologetically told him “grants are supposed to be free.” That’s when he realized it wasn’t real.

“They conned me out of my money, and the grant was a scam,” he says.

Corey went online to see if anyone else had experienced this. He read stories told by other people and learned they’d gone through the same thing, which gave him the courage to speak up.

“That inspired me—if these people can share their story, then I can too. I can help by warning others.”

What Corey wants you to know:

• If you’re receiving a real grant, you won’t be asked for money (especially not iTunes cards).
• “Always question everything, even if it doesn’t seem bad,” and use your best judgment and prior knowledge when somebody offers you something.

Additional tips from the BBB:

• Take a moment to check out the government agency offering the grant. The only official access point for all federal grant-making agencies is www.grants.gov.
• Phone numbers can deceive. Some con artists use Internet technology to disguise their identity and make it seem like they are calling from a government agency.

Data snapshot:

• Primary means of contact with monetary loss: phone
• Primary payment method: prepaid card

If you’re receiving a real grant, you won’t be asked for money (especially not iTunes cards).
The collection of self-reported demographic data such as age, gender and geographic location enhances our ability to identify those individuals most at risk and to understand how the nature of risk varies across different subgroups of the population. While we believe recognizing that we are all at risk is paramount, this information can be applied in targeting prevention efforts and informing outreach strategies.

**Age**

The data show a marked trend toward decreased susceptibility with increasing age (Figure 2). About 38 percent of individuals who provided age information when reporting to BBB Scam Tracker were 55 years of age or older, yet this group was far less likely to report a loss than the younger age groups.

While susceptibility declined with age, reported median losses increased (Figure 2). This may be a function of the types of scams different age groups are most susceptible to or are targeted by, or may be related to differences in access to financial resources with increasing age.

<table>
<thead>
<tr>
<th>AGE RANGE</th>
<th>TOP 3 MOST RISKY SCAM TYPES</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>Fake Check/Money Order</td>
</tr>
<tr>
<td></td>
<td>Online Purchase</td>
</tr>
<tr>
<td></td>
<td>Employment</td>
</tr>
<tr>
<td>25-34</td>
<td>Employment</td>
</tr>
<tr>
<td></td>
<td>Online Purchase</td>
</tr>
<tr>
<td></td>
<td>Advance Fee Loan</td>
</tr>
<tr>
<td>35-44</td>
<td>Online Purchase</td>
</tr>
<tr>
<td></td>
<td>Fake Check/Money Order</td>
</tr>
<tr>
<td></td>
<td>Advance Fee Loan</td>
</tr>
<tr>
<td>45-54</td>
<td>Investment</td>
</tr>
<tr>
<td></td>
<td>Online Purchase</td>
</tr>
<tr>
<td></td>
<td>Employment</td>
</tr>
<tr>
<td>55-64</td>
<td>Romance</td>
</tr>
<tr>
<td></td>
<td>Investment</td>
</tr>
<tr>
<td></td>
<td>Employment</td>
</tr>
<tr>
<td>65+</td>
<td>Tech Support</td>
</tr>
<tr>
<td></td>
<td>Family/Friend Emergency</td>
</tr>
<tr>
<td></td>
<td>Investment</td>
</tr>
</tbody>
</table>
Younger adults were more likely to fall for scams that used online means of contact (e.g., website, email, Internet messaging, online classifieds, social media, text message), while those 65+ years of age were more likely to fall for scams that used phone (Figure 3).

Younger adults were also more likely to pay via bank account debit, cash, or online payment systems, while older adults were more likely to use credit cards and checks (Figure 4).

---

12 Other category includes postal mail + other non-identified means of contact.
13 Other category includes non-identified payment methods.
Gender

Overall, women were nearly twice as likely to report a scam to BBB Scam Tracker as men. Contrary to last year, in 2017 women appeared to be slightly more susceptible to loss than men when exposed to a scam (Figure 5). However, median dollar losses for women remained substantially lower than for men (Figure 5). Similar to the differences in losses seen by age group, this may reflect gender differences in access to financial resources or differences in the types of scams that tend to impact men versus women. The BBB Risk Index formula has been applied to identify the top three riskiest scams by gender (Table 5).

![Figure 5: Susceptibility and Median Loss by Gender]

<table>
<thead>
<tr>
<th>GENDER</th>
<th>TOP 3 MOST RISKY SCAM TYPES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Women</td>
<td>Online Purchase</td>
</tr>
<tr>
<td>Men</td>
<td>Employment</td>
</tr>
</tbody>
</table>

Table 5: Top 3 Riskiest Scams by Gender
Geographic Area

Susceptibility, median loss, and the riskiest scams show some variability by region (Figure 6). This may be an indicator that the perpetrators of some types of fraud are more active in certain areas, and may also be a reflection of demographic and socio-economic differences by region that in turn correlate with differing levels of susceptibility and loss. It is important to note that these data refer to the location of the victim, not the perpetrator. While location information on perpetrators is provided in some cases, the accuracy of this information varies as most victims and targets are uncertain of the location of the perpetrator and are often given false information with respect to the fraudster’s location.

Figure 6: Most Risky Scam Types by Geographic Area

Western & Northern
- Median $ Loss: $270
- Most Risky Scam: Advance Fee Loan

Cananda
- Eastern
  - Median $ Loss: $231
  - Most Risky Scam: Advance Fee Loan

  1,477 (3.1%)
  Total Number of Reports

USA
- Midwest
  - Median $ Loss: $200
  - Most Risky Scam: Investment

- Northeast
  - Median $ Loss: $216
  - Most Risky Scam: Online Purchase

- Southeast
  - Median $ Loss: $220
  - Most Risky Scam: Online Purchase

- Southwest
  - Median $ Loss: $274
  - Most Risky Scam: Employment

- West
  - Median $ Loss: $250
  - Most Risky Scam: Employment

  46,350 (96.9%)
  Total Number of Reports
Fraudsters exploit the full range of communication channels to make contact with their targets, and readily adapt new communication methods or popular mediums. Figure 7 provides a comparison of all scam delivery methods reported to BBB Scam Tracker in 2017 where a monetary loss occurred. In 2017, website matched phone as the top means of contact for scams with monetary loss. Scams delivered by all of the various forms of online delivery (i.e., email, website, social media, online classifieds, Internet messaging) account for approximately 67 percent of all reports of monetary loss.

The range of payment methods used by scammers (Figure 8) is consistent with the variability and adaptability generally seen in the scam marketplace. However, criminals have an obvious interest in reducing or eliminating the likelihood that their transactions will be traced. For this reason, the use of payment methods such as wire transfers and gift cards are common, and should be considered a red flag for fraud.
It has long been recognized that military families and veterans are at increased risk of being targeted by scammers. The steady paychecks and relative youth of active-duty military personnel may make them particularly vulnerable. Individuals who self-identified as being active-duty military personnel, veterans or military spouses represent 8.6 percent of reports submitted to BBB Scam Tracker in 2017. These individuals may be more susceptible when exposed to a scam, with 17.5 percent reporting losses compared to 15.6 percent of non-military individuals. More striking is the median loss of $280, nearly 27 percent higher than the non-military median loss of $220 (Figure 9). The BBB Risk Index formula has been applied to identify the top three riskiest scams for military families and veterans (Table 6).

**Figure 9: Susceptibility and Median Loss by Military Families and Veterans vs. Non-Military**

<table>
<thead>
<tr>
<th>% Susceptibility</th>
<th>Median $ Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military</td>
<td>17.5%</td>
</tr>
<tr>
<td>Non-Military</td>
<td>15.6%</td>
</tr>
</tbody>
</table>

**Table 6: Top 3 Scams: Military Families and Veterans vs. Non-Military**

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>TOP 3 MOST RISKY SCAM TYPES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military/Veterans</td>
<td>Employment, Home Improvement, Online Purchase</td>
</tr>
<tr>
<td>Non-Military</td>
<td>Online Purchase, Investment, Employment</td>
</tr>
</tbody>
</table>
SPOTLIGHT ON STUDENTS

Individuals who self-identified as students represent 7.6 percent of reports submitted to BBB Scam Tracker in 2017. These individuals appear to be significantly more vulnerable when exposed to a scam: 25.1 percent of students reported a loss as compared to 15 percent of non-students (Figure 10). However, the median dollar loss of $200 for this group is significantly lower than the median loss for non-students of $231 (Figure 10). This may reflect differences in the scam types to which students are most vulnerable, as well as differences in access to funds (Table 7). It should also be noted that the susceptibility rate and median losses for students are very similar to those of the overall 18-24 age category into which most students fall.

Figure 10: Susceptibility and Median Loss for Students

<table>
<thead>
<tr>
<th>% Susceptibility</th>
<th>Median $ Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Students</td>
<td>15.0%</td>
</tr>
<tr>
<td>Students</td>
<td>25.1%</td>
</tr>
</tbody>
</table>

Table 7: Top 3 Scams: Students vs. Non-Students

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>TOP 3 MOST RISKY SCAM TYPES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students</td>
<td>Employment</td>
</tr>
<tr>
<td>Non-Students</td>
<td>Online Purchase</td>
</tr>
</tbody>
</table>
“Impersonation” is a very common tactic used by scammers. It’s where the scammer pretends to be a legitimate business that is well known and trusted by the consumer. Here’s an example:

“On the driver’s license renewal site for Tennessee, there is a huge advertisement from getdriverslicense.com. It is very misleading, causing you to think that this is part of the original site. I clicked on it to get a replacement drivers license, filling out all my info and credit card info. I was charged $25 thinking it was for a driver’s license, but it was only for a pamphlet telling me to go to the DMV.”

Impersonations are utilized for a variety of scams:
- Tech support scams (the scammer pretends to be a well-known technology company such as Microsoft, Apple, etc.)
- IRS scams (the scammer pretends to be the IRS or Canada Revenue Agency)
- Bank scams (the scammer pretends to be a well-known financial institution such as Bank of America or Capital One, etc.)
- Government grant scams (the scammer pretends to be a government agency)
- Travel/vacation scams (the scammer pretends to be a well-known travel “brand” such as Marriott or Trip Advisor.)

While all scammers pretend to be some sort of legitimate operation by definition, this particular tactic is where the scammer pretends to be a known, trusted entity like Bank of America, Capital One, Apple, Facebook, Microsoft, or the Internal Revenue Service. Table 8 below highlights the top 15 legitimate organizations that were used by scammers in their impersonation tactics.

Table 8: Top 15 Legitimate Organizations Used for Impersonation

<table>
<thead>
<tr>
<th>Rank</th>
<th>Organization</th>
<th>Scams</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>U.S. Internal Revenue Service</td>
<td>2,103</td>
</tr>
<tr>
<td>2</td>
<td>U.S. Government (Grant/Treasury/Reserve/Medicare)</td>
<td>985</td>
</tr>
<tr>
<td>3</td>
<td>Better Business Bureau</td>
<td>628</td>
</tr>
<tr>
<td>4</td>
<td>Publishers Clearing House</td>
<td>584</td>
</tr>
<tr>
<td>5</td>
<td>Microsoft</td>
<td>517</td>
</tr>
<tr>
<td>6</td>
<td>Apple</td>
<td>173</td>
</tr>
<tr>
<td>7</td>
<td>Marriott</td>
<td>131</td>
</tr>
<tr>
<td>8</td>
<td>TripAdvisor</td>
<td>109</td>
</tr>
<tr>
<td>9</td>
<td>Canada Revenue Agency</td>
<td>99</td>
</tr>
<tr>
<td>10</td>
<td>Facebook</td>
<td>82</td>
</tr>
<tr>
<td>11</td>
<td>Advance America</td>
<td>54</td>
</tr>
<tr>
<td>12</td>
<td>Bank of America</td>
<td>48</td>
</tr>
<tr>
<td>13</td>
<td>PayPal</td>
<td>48</td>
</tr>
<tr>
<td>14</td>
<td>Capital One</td>
<td>47</td>
</tr>
<tr>
<td>15</td>
<td>Yellow Pages</td>
<td>43</td>
</tr>
</tbody>
</table>
While scams abound, scammers do not always succeed in claiming a victim. In fact, 84.2 percent of the reports to BBB Scam Tracker in 2017 were from non-victims. Fighting back and passing on the message to help others is important. In an effort to support that movement, we share below a few tips on how to spot a scam. We also share below an initiative from the BBB Serving Wisconsin that proved very successful in 2017.

**Learn How to Spot a Scam**

There are several new scams every year, and it’s difficult to keep up with all of them. But if you can just remember these 10 things, you can avoid most scams and help protect yourself and your family.

1. **Never send money to someone you have never met face-to-face.**
2. **Don’t click on links or open attachments in unsolicited email.**
3. **Don't believe everything you see.** Scammers are great at mimicking official seals, fonts, and other details. Just because a website or email looks official does not mean that it is. Even Caller ID can be faked.
4. **Don't buy online unless the transaction is secure.** Make sure the website has “https” in the URL (the extra s is for “secure”) and a small lock icon on the address bar.
5. **Be extremely cautious when dealing with anyone you’ve met online.**
6. **Never share personally identifiable information with someone who has contacted you unsolicited.**
7. **Don't be pressured to act immediately.**
8. **Use secure, traceable payment methods** when making payments for goods, services, and taxes.
9. **Whenever possible, work with businesses** that have proper identification, licensing, and insurance.
10. **Be cautious about what you share on social media.**

Get further details online at [BBB.org/AvoidScams](http://BBB.org/AvoidScams)

**Payback Time: Wisconsin BBB Calls the Scammers**

What if you had the opportunity to pay back scammers? This is what the BBB Serving Wisconsin is doing in a series of videos in which they call the scammers and pretend to be a potential victim. It is #PaybackTime and you can see the most-viewed video to date: “IRS Scammer Gets Called by BBB”: [BBB.org/Payback](http://BBB.org/Payback)
For the third consecutive year, the BBB Institute for Marketplace Trust has delivered new and timely research about scams. In 2016, we published a primary research paper, “Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias and the Way Forward for Marketplace Scam Education.” The paper, available at BBB.org/TruthAboutScams, offered key findings and recommendations based on a survey of more than 2,000 adults in the United States and Canada, as well as BBB Scam Tracker report data. The paper was the first to survey the public to explore consumer perceptions and stereotypes about scam victims. Importantly, we found that these perceptions are often inaccurate and can contribute to a false sense of invulnerability.

Other notable findings from this study:

- Younger and more educated individuals are more likely to report losing money to a scam than those who are older and less educated.
- Information about current scam types and the tactics used by scammers were cited as being the most important factors in helping individuals targeted by scams to avoid becoming a victim.
- When individuals choose to report a scam, they are most often motivated by a desire to warn others, rather than recovering lost funds or bringing the perpetrator to justice.
- U.S. respondents identified BBB as the top of mind resource for reporting scams, and second only to Google for researching scams.14

The 2016 Risk Report provided a meaningful glimpse of the scam landscape, informing future BBB educational efforts and outreach.

The report garnered a great deal of attention from the media, the government and like-minded consumer-protection groups. The BBB Institute testified before the U.S. Senate Special Committee on Aging regarding scams and older Americans. We were also invited to present before several organizations, including the Communications Fraud Control Association, the 2017 National Aging and Law Conference organized by the American Bar Association, the Consumer Federation of America, the National Cyber-Forensics and Training Alliance, and the American Bankers Association.

With the publication of the second report and additional research on the horizon, we will continue to add fresh perspectives and more detailed data to the scam and fraud landscape.

14 https://www.bbb.org/truth-about-scams/
The BBB Risk index introduced the notion that scam risk is a multi-dimensional construct. We can more accurately assess the risk and impact of the massive number of scams in the marketplace by using the quantifiable factors of exposure, susceptibility, and monetary loss (see Figure 11 for Top 10 Riskiest Scams). But just as there is no single scam type or method, there is no single set of factors that can determine scam risk in all cases. Depending on the problem, the factors in the template we have developed could be further refined; each factor could be weighted differently; and other factors could be introduced to calibrate risk in a more granular way. We invite other organizations, researchers and government entities engaged in the fight against scams to join with us to further our work in this area.

To date, the Risk Report has focused on determining the relative risk of particular scam types. There are other factors that we have touched on in our reports that merit further study. Measuring externalities that are not currently part of scam risk analysis would yield valuable insight into the overall cost of scams to society. While these factors may be more difficult to quantify than those that we are currently including in our risk analysis, we need to find ways to measure and include them.

For example, technology has reduced scammers’ costs in contacting consumers. Our email inboxes are flooded with phishing scams of one type or another. Our phones are flooded with scam robocalls that spoof our local numbers and fool Caller ID. Even though autodialed scam calls have a relatively low success rate, they have other economic costs. We sense that scammers’ use of robocalls is more than an annoyance. It is degrading the trust and usefulness of telephone calls in the marketplace and negatively affecting consumers and the legitimate businesses and other entities that can no longer rely on consumers to pick up the phone.

Other non-monetary losses are a significant part of the damage that scams cause. While it is much more difficult to quantify or measure, the emotional toll of scams can be devastating. These effects can include feelings of helplessness and depression, as well as anxiety, shame, sleeplessness or suicidal thoughts. More work needs to be done to understand and measure these effects.

Identifying and quantifying the human dimension of scam risk and impact is also essential to developing an accurate picture of scam risk and how to reduce it. In the Invulnerability Illusion report, the BBB Institute conducted survey research into people’s beliefs about scams. An analysis of the resulting data challenged traditional notions of scam victimology. It replaced the stereotype of the gullible and uneducated person, most often a senior citizen, as the typical scam victim, with data that demonstrated that the most frequent victims are in fact millennials, and that victims tend to be highly educated and prosperous.

Seniors, in fact, fell victim to scams less frequently. One of the most powerful and overlooked factors in

If we can understand more precisely how scam loss affects its victims, we can increase the effectiveness of the initiatives we undertake to help victims of scams.

LOOKING FORWARD

determining scam risk is the psychology of invulnerability. The less likely people think they are to be fooled by a scammer, the greater their risk of becoming a victim. Much more can be gleaned from these insights.

To fight scams successfully, educational efforts must look at the scam vulnerabilities of each cohort with regard to scam type and the psychology of scammer and victim. Our messaging must pose the paradox—the more you think you can’t be conned, the more likely you are to be a victim. BBB Scam Tracker works to defang embarrassment, empower consumer action and encourage peer-to-peer awareness. If we can understand more precisely how scam loss affects its victims, we can increase the effectiveness of the initiatives we undertake to help victims of scams.

Consumers—Learn About and Report Scams
Help us continue the fight against scammers and fraudsters. Visit the BBB Scam Tracker website at BBB.org/ScamTracker to learn about and report scams. Every person who contributes to this effort helps to prevent additional victims and advances our collective knowledge and understanding of this problem.

Businesses—Join Us as We Create Best Practices for Preventing Scams
The BBB Institute believes by working together, businesses can play an important role in building trust between consumers and good businesses and defeating scammers. For this reason, we created the Corporate Trust Roundtable, a unique forum for business leaders to discuss and develop initiatives that address critical marketplace issues. Businesses interested in learning more should contact us at Institute@council.bbb.org.

Researchers—Help Us Expand Our Scam Research
The BBB Institute is partnering with university researchers, foundations and think tanks to produce cutting-edge research. We invite collaboration on the issues discussed in this report and on other research projects focused on 21st century marketplace issues.

**Take Action Today**
We thank the thousands of individuals and businesses who made this report possible by reporting scams to BBB Scam Tracker. Together, we will continue to make a difference in the fight against marketplace scams.
CONCLUSION

In order to thrive and prosper, consumers and businesses must be able to operate in a fair and transparent marketplace. Scammers undermine trust in the marketplace, distorting the level playing field and siphoning off money from legitimate transactions that benefit both businesses and consumers, thus impeding economic growth. A consumer who has been scammed not only has fewer dollars to spend in the market, but may also shy away from normal engagement in commerce. A business whose trustworthy brand has been impersonated by scammers may find consumers’ trust in its brand diminished.

The 2017 Scam Tracker Annual Risk Report is an important landmark in ongoing work to contribute new, useful data and analysis to further the efforts of all who are engaged in combatting marketplace scams. It marks a critical next step in providing timely information, data continuity, and fresh insight about scams in the marketplace. We will continue our work to fight scams to help consumers and legitimate businesses prosper in a trustworthy marketplace.
APPENDIX A: GLOSSARY OF SCAM TYPE DEFINITIONS

Scams reported to BBB Scam Tracker are classified into 30 scam types. These classifications represent common scams seen by BBB over time, and are also informed by type classifications used by the Federal Trade Commission and the Internet Crime Complaint Center of the Federal Bureau of Investigation. While scams vary widely, approximately 90 percent of all scams reported to BBB Scam Tracker can be classified into one of these general types.

<table>
<thead>
<tr>
<th>Scam Types</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advance Fee Loan Scams</td>
<td>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.</td>
</tr>
<tr>
<td>Business Email Compromise Scams</td>
<td>This financial fraud targets businesses engaged in international commerce. Scammers gain access to company email and trick employees into sending money to a “supplier” or “business partner” overseas.</td>
</tr>
<tr>
<td>Charity Scams</td>
<td>Charity scams use deception to get money from individuals believing they are making donations to legitimate charities. This is particularly common in the wake of a natural disaster or other tragedy.</td>
</tr>
<tr>
<td>Counterfeit Product Scams</td>
<td>Counterfeit goods mimic original merchandise, right down to the trademarked logo, but are typically of inferior quality. This can result in a life-threatening health or safety hazard when the counterfeit item is medication or an auto part.</td>
</tr>
<tr>
<td>Credit Card Scams</td>
<td>This con typically involves impersonation of a bank or other credit card issuer. By verifying account information, con artists try to fool their targets into sharing credit card or banking information.</td>
</tr>
<tr>
<td>Credit Repair/Debt Relief Scams</td>
<td>Scammers posing as legitimate service providers collect payment in advance with promises of debt relief and repaired credit, but provide little or nothing in return.</td>
</tr>
<tr>
<td>Debt Collection Scams</td>
<td>In this con, phony debt collectors harass their targets, trying to get them to pay debts they don’t owe.</td>
</tr>
<tr>
<td>Employment Scams</td>
<td>Victims of employment scams are led to believe they are applying or have just been hired for a promising new career while they have, in fact, given personal information or money to scammers for “training” or “equipment.” In another variation, the victim may be “overpaid” with a fake check and asked to wire back the difference.</td>
</tr>
<tr>
<td>Fake Check/Money Order Scams</td>
<td>In this con, 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.</td>
</tr>
<tr>
<td>Fake Invoice Scams</td>
<td>This scam targets businesses. Scammers attempt to fool employees into paying for products that the business did not order and that may not even exist. Fake invoices are often for office supplies, website or domain hosting services, and directory listings.</td>
</tr>
<tr>
<td>Family/Friend Emergency Scams</td>
<td>This scheme involves the impersonation of a friend or family member in a fabricated urgent or dire situation. The “loved one” invariably pleads for money to be sent immediately. Aided by personal details they’ve found on social media, imposters can offer very plausible stories to convince their targets.</td>
</tr>
<tr>
<td>Foreign Money Exchange Scams</td>
<td>In this scam, the target receives an email from a government official, member of royalty, or a business owner offering a huge sum for help getting money out of their country. The victim fronts costs for the transfer, believing that they will be repaid.</td>
</tr>
<tr>
<td>Government Grant Scams</td>
<td>In this con, 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.</td>
</tr>
<tr>
<td>Health Care, Medicaid and Medicare Scams</td>
<td>These schemes run the gamut, with many attempting to defraud private or government health care programs. The con artist is often after the insured’s health insurance, Medicaid, or Medicare information to submit fraudulent medical charges or for purposes of identity theft.</td>
</tr>
<tr>
<td>Scam Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Home Improvement Scams</strong></td>
<td>In this con, door-to-door solicitors offer quick, low-cost repairs and then either take payments without returning, do shoddy work or “find” issues that dramatically raise the price.</td>
</tr>
<tr>
<td><strong>Identity Theft Scams</strong></td>
<td>Identity thieves use personal information (e.g., Social Security Number, bank account information, and credit card numbers) to pose as another individual for their own gain. This may include opening a credit account, draining an existing account, filing tax returns or obtaining medical coverage.</td>
</tr>
<tr>
<td><strong>Investment Scams</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Moving Scams</strong></td>
<td>These schemes involve rogue moving services offering discounted pricing to move household items. They may steal the items or hold them hostage, demanding additional funds to deliver them to the new location.</td>
</tr>
<tr>
<td><strong>Online Purchase Scams</strong></td>
<td>These cons often 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.</td>
</tr>
<tr>
<td><strong>Phishing Scams</strong></td>
<td>These schemes employ communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information or passwords.</td>
</tr>
<tr>
<td><strong>Rental Scams</strong></td>
<td>Phony ads are placed for rental properties that ask for upfront payments. Victims later discover the property doesn’t exist or is owned by someone else.</td>
</tr>
<tr>
<td><strong>Romance Scams</strong></td>
<td>An individual believing he/she is in a romantic relationship is tricked into sending money, personal and financial information, or items of value to the perpetrator.</td>
</tr>
<tr>
<td><strong>Scholarship Scams</strong></td>
<td>This con hooks victims, often students struggling with tuition costs, with the promise of government scholarship money, but the upfront “fees” never produce those much-needed funds. Sometimes a fake check does arrive, and the student is asked to wire back a portion for taxes or other charges.</td>
</tr>
<tr>
<td><strong>Sweepstakes, Lottery and Prize Scams</strong></td>
<td>In this con, imposters pose as Internal Revenue Service representatives in the United States or Canada Revenue Agency representatives in Canada to coerce the target into either paying up or sharing personal information.</td>
</tr>
<tr>
<td><strong>Tax Collection Scams</strong></td>
<td>Tech support scams start with a call or popup 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.</td>
</tr>
<tr>
<td><strong>Tech Support Scams</strong></td>
<td>Con artists 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.</td>
</tr>
<tr>
<td><strong>Travel and Vacation Scams</strong></td>
<td>In this con, scammers impersonate water, electric and gas company representatives to take money or personal information. They frequently threaten residents and business owners with deactivation of service unless they pay immediately. In another form, a “representative” may come to the door to perform “repairs” or an “energy audit” with the intent of stealing valuables.</td>
</tr>
<tr>
<td><strong>Utility Scams</strong></td>
<td>This con targets businesses, attempting to fool them into paying for a listing or ad space in a non-existent directory or “Yellow Pages.” In some cases, the directory will technically exist, but will not be widely distributed and a listing will be of little or no value—these directories are essentially props in the scammer’s ploy.</td>
</tr>
<tr>
<td>Scam Types</td>
<td># of Reports</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Advance Fee Loan</td>
<td>1,061</td>
</tr>
<tr>
<td>Business Email Compromise</td>
<td>222</td>
</tr>
<tr>
<td>Charity</td>
<td>419</td>
</tr>
<tr>
<td>Counterfeit Product</td>
<td>886</td>
</tr>
<tr>
<td>Credit Card</td>
<td>1,244</td>
</tr>
<tr>
<td>Credit Repair/Debt Relief</td>
<td>572</td>
</tr>
<tr>
<td>Debt Collection</td>
<td>2,304</td>
</tr>
<tr>
<td>Employment</td>
<td>2,429</td>
</tr>
<tr>
<td>Fake Check/Money Order</td>
<td>1,097</td>
</tr>
<tr>
<td>Fake Invoice</td>
<td>814</td>
</tr>
<tr>
<td>Family/Friend Emergency</td>
<td>341</td>
</tr>
<tr>
<td>Foreign Money Exchange</td>
<td>128</td>
</tr>
<tr>
<td>Government Grant</td>
<td>1,981</td>
</tr>
<tr>
<td>Health Care, Medicaid, and Medicare</td>
<td>646</td>
</tr>
<tr>
<td>Home Improvement</td>
<td>374</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>886</td>
</tr>
<tr>
<td>Investment</td>
<td>238</td>
</tr>
<tr>
<td>Moving</td>
<td>64</td>
</tr>
<tr>
<td>Online Purchase</td>
<td>4,655</td>
</tr>
<tr>
<td>Phishing</td>
<td>13,774</td>
</tr>
<tr>
<td>Rental</td>
<td>295</td>
</tr>
<tr>
<td>Romance</td>
<td>144</td>
</tr>
<tr>
<td>Scholarship</td>
<td>15</td>
</tr>
<tr>
<td>Sweepstakes, Lottery and Prize</td>
<td>2,820</td>
</tr>
<tr>
<td>Tax Collection</td>
<td>3,090</td>
</tr>
<tr>
<td>Tech Support</td>
<td>2,277</td>
</tr>
<tr>
<td>Travel and Vacation</td>
<td>2,560</td>
</tr>
<tr>
<td>Utility</td>
<td>500</td>
</tr>
<tr>
<td>Yellow Pages/Directories</td>
<td>165</td>
</tr>
<tr>
<td>Other</td>
<td>1,826</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>47,827</strong></td>
</tr>
</tbody>
</table>
## The Victims Index

### #1 Online Purchase Scams

**Alabama**
I went to a website to try and buy a car. When I emailed the seller, they emailed me back saying, “The car is for sale for $6,100. The car is being sold as described. I am working overseas with [Exxon Mobil] and my contract is over [in] October 2017. If you want more details I need you to register with my shipper in Portland Oregon, which is where the car is. They are Williams Transport and at www.williams-trans.com and will be safe for both of us. They will take the money and hold it until you receive the car. You will then have 7 days to look over the car...” They then wanted me to wire transfer it, so I called the Better Business Bureau. They let me know that there is no valid business license for this company. I asked the company to show me a valid business license and I haven’t heard from them since so I know it’s a scam.

**Colorado**
I picked out a TEA CUP SHIH TZU puppy from the website listed above from a man supposedly named “Mr. Thomas Marrel” for $500. He asked me to pay for the puppy via Western Union, which I did.... A couple of days later he “tried” to scam me out of MORE MONEY by telling me that the shipping company that would fly the puppy to me needed $450 MORE dollars from me for insurance. This money was 100% refundable and would be given back to me UPON delivery of the puppy in hand. I did actually try to send this money, but after numerous excuses [for] why the puppy was not being delivered.... I called Western Union and CANCELLED the transaction BEFORE this new person “Mr. James Marcot” at the SAME address as above .... was able to pick up the money due to the X-mas holiday. This company and this man are a SCAM!!!!! And he has stolen $500 from me and I have NEVER received a puppy or another call or email from him.

**Georgia**
I ordered a dress from this website in September, never to receive it. A few months later, I emailed them to get a refund and they claimed they would reward it to me. Fast forward to 2 weeks ago; they sent me an email (after I had sent 3 other emails regarding my supposed refund) claiming that they rewarded me with a full refund. I have kept track of my account that I purchased my dress on and they have yet to refund me. This website has done the same thing to many other people I know personally as well as people I have seen complaining about it on [Google.] This website is a scam to filter money from unsuspecting customers and then they do not send the product nor give a refund when requested.

### #2 Investment Scams

**California**
This is a complete scam designed to scare elderly people to use their retirement funds to buy gold and silver that is completely over-valued by the company. When we researched the gold my grandmother had purchased through them we found that it was twice the cost of market value. She essentially lost half of her retirement savings.

**Wisconsin**
Over the past few weeks [my] grandfather was contacted by someone from 917-563-2384 and was on the phone for a long time. Today, he was rushed to the hospital due to his diabetes and he would not give up the phone. He kept getting calls and saying ‘give me my funds.’ We thought this was odd and after doing some checking it looks like he has given someone most of his money. We found out that my grandfather asked my sister to drive him to the bank and to FedEx and told her not to tell anyone. I got his phone and found the number and called it. When I asked what business this was he said it was the FBI & his name was Jacob Wright. I asked where he was located and he said in Chicago. When I asked for the address he said he would only give me the location when I got into Illinois. I was back at the house when the landline rang and it was the same person, but this time his name was John Green. We are trying to figure out how much was lost and who these people are.
### THE VICTIMS INDEX

<table>
<thead>
<tr>
<th>#2 INVESTMENT SCAMS</th>
<th>BRITISH COLUMBIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>We were invited to attend a presentation with other families to look at a great fundraising opportunity for a team. It turned out to be a presentation for a pyramid scheme called ‘Pay It Forward’ (a gifting circle). The presentation began by advising that no recording (video or audio) [is] allowed and next tells you that [it] is not a pyramid scheme and is 100% legal (all this before they tell you what is involved, this was the first Red Flag for me). You are encouraged to join on the baseline and hand over your gift of $5,000 (when you have the money available) and recruit two more people (who then recruit 2, etc., or you can share a spot with someone and split the investment) in order to climb to the top and receive a $40,000 ‘Birthday Gift’. There are only 15 people in a “Cloud”; as people are recruited the Clouds split off to new clouds and this is how you reach the top position…. We were also told that we are not to tell anyone the details of the presentation as there are people in the program (i.e., celebrities, famous sports players etc) who don’t want anyone to find out about their involvement as they are doing it to help others to also make money. We were also advised not to run home and “Google” it because the Blogs that come up contain the information that is not fact based…. They also advise it is 100% legal because there is no “Treasurer”; money changes hands directly between parties. When it is your turn to receive a “Birthday Gift” you purchase $50 gift cards to exchange with the people you receive gifts from. If we chose to become involved we were told to email our information (Name, Phone, Email &amp; Cloud Name) to the person that invited us and we would then be asked to download the “Telegram” App in order to communicate in the Cloud Chats. We recognized this for the scam it is, however are concerned because other families were excited at the possibility of making easy money.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#3 EMPLOYMENT SCAMS</th>
<th>CALIFORNIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>I was first contacted via telephone by this “staffing company” that had found my resume online. They told me they had a job opportunity through the county available for me. I would just need to email them my I-9s, and fill out a TB test, and I would be contacted by someone to make an appointment to finish the testing, as required by the county. I naively sent my I-9s (personal info) via email, and filled out the request form. I was told I would be reached out [to] by someone within 72 hours. 72 hours passed, and I received no contact from the agency, nor any establishment that did testing. I contacted my staffing agent via email stating I had not received a call, and she’s replied saying she would contact them right away to get things sorted out. Over a week later, I still did not receive a call from either party. I called the main office only to be given the runaround about what was going on…. I was called back and told that the information was already given to me. I TRIPELe checked all of my emails, and I never received any reply from anyone regarding a contact number for this TB testing facility. I became upset and told them I felt like I was being played for a fool, and would be filing a complaint. I had given my personal information, via an unsecured source, and was worried about identity theft. I was then told by a manager they would shred my information. I informed them I gave them the information via EMAIL, which was/is unsecure and there would be no way to shred the info. It was now available for anyone to see. I feel foolish for having given up my information so easily, but it’s a lesson learned.</td>
<td></td>
</tr>
</tbody>
</table>
## THE VICTIMS INDEX

### MISSOURI

Fortunately, I think I caught on before giving too much information. I had put an ad on Craigslist about being willing to tutor. This person contacted me saying his 8-year-old boy needed help in Algebra. He asked what experience I had, and I told him, listing some schools I had taught at. He said I sounded competent, and wanted me [to] tutor his son, even giving me a choice at my house or in a public place like the library or coffee shop. Sounded good—however, when I said I wanted to meet with him, he said he was out of the country, and his lawyer needed info to send me the check for the hours he wanted me to tutor. (His son’s caregiver lived near me, he said.) I got suspicious when he asked for my name and address, where to send the check, even though we hadn’t met. I told him I would not be comfortable getting a check from him before meeting with him, and if he would like to meet with me when he returned later in the summer, maybe that was possible. I have not heard from him since.

### TEXAS

I was contacted by Christie Anderson with this company for a job position as a Senior Buyer. She sent me an application that looked like it came from Microsoft Word with floral print on it. Though it looked unprofessional, I proceeded to fill it out because the job promised a salary of $86,400.00. After submitting the application, I received a phone call from Christie days later for a phone interview…. The phone interview was very short. She asked me what I did at my current employer and when would I be available to start. I told her, asap if I could work remotely. She told me I sounded like the perfect person for the job and I would hear back from her Monday. That following Wednesday, I got an email stating I “passed,” and they want to work with me. Christie sent a lengthy email stating my job description and sent me an employment agreement to sign. This looked like it was downloaded off the internet and stated it was governed by “Missouri Law” even though the company is based in Mississippi, which was another red flag, but I proceeded to go with it. The next day I received new hire documents from Christie to fill out and return which included W-4, I-9 and a Direct Deposit form. I filled out everything also sending copies of my social and ID. The next day I received an email from Christie asking for my credit report. This is when I became alarmed. I almost sent her a copy; then she emailed me again asking for my credit karma login and password. I tried to call her and the phone immediately went to voicemail. I looked up the number and it states it’s a VOIP number like [Google Voice] and the business address is an apartment complex. Then I realized I never applied to this company so I’m not sure how they got my email address….This is a scam to steal people’s identity with voluntary info we provide thinking it’s for employment.

### FLORIDA

I got an email from a Charles Becker claiming to be from Ace Cash Express saying I had applied and been approved for an $8000.00 installment loan. I immediately emailed back the word SCAM. He then replied with a PDF file of loan papers. They actually had company letterhead and all. I called the number and it was a man of foreign descent who demanded my name. I gave him a fake name. He proceeded to tell me I needed to go purchase a prepaid card and load $500.00 on it in order for them to deposit this so-called loan in my bank account. Of course he wanted all my info, name, ss, bank info, address etc... I’m actually getting up to 10 scam calls daily ranging from “IRS” to phishing. I have been living [with] and taking care of my 89-year-old mother-in-law over 10 years, and of course the home phone is in her name. This has got to stop. These scammers put the fear of God in these elderly people and make serious threats of being arrested, felony charges and so many awful things. If my husband and I were not here, she would literally give them everything they asked for out of fear. This has to stop. Elderly people shouldn’t have to worry about this.
## THE VICTIMS INDEX

| GEORGIA | I was dealing with financial hardship at the time, needing help with bills. I went online to apply for a loan. I received a message by phone stating that this company would possibly be able to help me with my situation. I thought, “thank you, Lord; finally I can stop crying every night and waking up and pretending nothing was wrong to my children and others.” Upon speaking with the rep from the loan company they broke down how I would pay them back. I’ve never done this before so I really didn’t know the ins and outs and how it all worked. I just wanted some help for bills...so as we proceeded with the loan process he then stated that I should put some type of insurance on the loan to cover myself, God forbid anything were to happen to me and I was unable to make payments. So I did. I put all of the money that I had left to my name down as insurance coverage for my loan. I asked him, “What form of payments do you accept?” He stated [Western Union] and another company... and iTunes cards. He stated that in order to speed up the process of getting my loan, it [would] be best for me to make my payments through “iTunes cards.” So being the desperate, gullible me in my crisis and need of help—never dawning on me this is a scam—I proceeded. Because in my heart all I was looking for was some financial help with my bills; not to be a part of any illegal activity. This company took all the money from me that I had left. I could have put the money for my “insurance” towards bills and just continued to try and come up with more money. I gave them all of my personal information... [The rep said he’d] wire money into...[my] account as verification money and then I’d have to send it back to them. So I said, [Ok, and all I have to do is get the money back to you all and my loan will be taken care of.]” He said, “Yes, because it’s just to make sure your account is in good standing,” or something of that nature. So I did just so and this all had to be done through “iTunes cards.”...Upon trying [to] retrieve the money is when I found out it was all a scam. I spoke to the branch manager trying to get a manual release on my money, only to find out that these people [deposited]...a fake check into my account. |

| MASSACHUSETTS | [They] contacted me via email about a personal loan. Due to my poor credit, they wanted a down payment. They sent a contract with a step-by-step explanation of how you will receive your money if you follow the simple steps. Three months of payments and you get [an] $8,000 loan. I paid up front $591. Waiting two hours for the deposit into my account. Then they said I need insurance, normally $1,500 but they could do $750, but it would be refunded in three months. So I took my mortgage payment and paid it to them because they said in two hours $8,000 would be in my account. Again it wasn’t. [Then they stated] that they really needed the other $750, to make it work. I didn’t have it, and demanded my money back. They said they would, after a small processing fee; and I would receive it on 5/26/17. Well, that day has come and gone, and no refund. Please people send no money to anyone. |

| CALIFORNIA | Buyer offered full price [for furniture] and promised to send [a] cashier’s check for amount, but noted [they] would send extra money for “pickup.” Sale amount [was] $1,200. Check received [was] not [a] cashier’s check, but I did not notice. Check was for $2,355.14. [I] immediately cashed check with my bank. Buyer sent email instructions directing me [to] deposit excess back to provided bank account. Did as directed. Delays from buyer stating family hardship. After buyer acknowledged receipt of $1,155.14, [he continued] delays for my request for contact information. After more delay, [I] was informed by buyer that he wanted to cancel sale due to death in family and asked for remaining $1,200 to be sent back. I refused this. Finally received notice from bank that check for $2,355.14 was fraudulent and my account was debited for the full amount. I am now out $1,155.14 that I will likely never see again. |

## #4 ADVANCE FEE LOAN SCAMS

## #5 FAKE CHECK/MONEY ORDER SCAMS
#5 FAKE CHECK/MONEY ORDER SCAMS

**LOUISIANA**

Received what seemed like a legit email from Survey Monkey, with Walmart name. Was told [I] was to do a shopping survey. [One] week or so later I received another email confirming that I wanted to do it and told me to watch my mail. Two days later I received a check for $1,800. It told me to deposit it in my account and wait 24 hours and then deduct $300 for my time and then buy something for no more than $50, noting cashier’s name and everything about her. Then told me to wire $1,450 to a Patricia Filoteo, Bakersville, CA. It told me if they asked if I knew her to say yes. Then I was to take the number and email and text it to derrickoffice101@imageofficesurvey.com and text to (707)403-2336. It made sure to tell me not to alert anyone of what I was doing. Just all sounded creepy. I let my police officer husband read it and he said, check BBB; sure enough, several of the same type of complaint[s,] just different names. I tore up the check and will have nothing further to do with these people.

**TENNESSEE**

The letter I received via regular US Postal Service was in a cheap, over-sized, express delivery envelope; it read as follows: Secret Shopper Number #8440 Survey and Research Document section 4 batch A / 2017. On receipt of this letter you are to text message 636-730-5322 to acknowledge you received this package. It is important that you remain discrete. Read instructions carefully: If asked if you know the recipient say yes. If asked if you are a secret shopper say no. Locate a Western Union and Money Gram store nearest you. This envelope contains a cashier’s check for 1,980.00. You are to have the check cashed at your bank. Once you have withdrawn the cash from your bank, immediately send a text to smithsim977@gmail.com. Once you have transferred 800.00 at Western Union and 800.00 at Money Gram you are then expected to complete this assignment as soon as possible: send text to 636-730-5322 confirming completion. Then send email with the transfer details. Name and Address of Sender. Money Gram transfer number and Western Union transfer number. Here is all the information needed to send both transfers. Also you are to confirm the receipt for spelling mistakes of the receiving secret shopper name…. I HAVE THE CHECK AND THE LETTER ON FILE AND AM REPORTING IT TO LOCAL POLICE.

#6 HOME IMPROVEMENT SCAMS

**ILLINOIS**

I was referred by Total Home Protection; they scheduled me [Name withheld] to do some plumbing work. He called to schedule the appointment., and asked to be paid in advance through PayPal. I paid JMorgan contractors $125.00 through PayPal in advance. He never came to do the work. [Stopped] answering his phone. Total Home Protection had to send out another company to do the work. Never got my deductible ($125.00) back. He is a scammer. He owes me $125.00, of which he got an advance payment for service he never did. Beware of JMorgan Contractors. I need my money. I am a senior citizen.

**NEW YORK**

MPG Maintenance Corp., aka Michael Guarino...also possibly operates under “Chimney Cleaners,” contacted my elderly father for chimney service he didn't need on 8/1/17 & again on 11/17/17. The first time he got my father for $2,750 & the second time for $3,250. Mr. Guarino cashes the checks immediately after being paid. My family is positive my father didn’t need the chimney work. After finding out about the second time...unfortunately too late, I researched Michael Guarino on the internet & found he was arrested for fraudulent chimney service in Connecticut & New Jersey back in 2012....
#6 HOME IMPROVEMENT SCAMS

**MINNESOTA**
Received a flyer for Metro Guys Landscaping—I called to get an estimate. Jeff Ekdahl came out to my home and gave me an estimate for the fence repair. They did part of the job and told me that they only had a little left to do. The estimate was way too low because of the “extra work” they had to do to dig out the cement where the replacement post had to go. Jeff had to run to get additional brackets and since I was leaving asked if I’d pay them so they did not have to make another trip back. I FOOLISHLY paid him. He immediately went to my bank and cashed the check and has never returned. Keeps telling me he is coming to finish the work.

#7 TECH SUPPORT SCAMS

**NEW YORK**
I was searching on the internet for a short movie for my son. A warning of a virus popped up on my computer. I tried closing the browser, running the antivirus software and shutting off the computer. Nothing worked, so I called the phone number on the warning, believing it was an official tech service number. The tech stated he needed to access my computer remotely in order to assess the problem. He had me type in “iexplore helpme.net” to gain access to my computer. Once in, I was told and shown on the computer that my antivirus software was an old version that didn’t work with Windows 10. I was shown and told my IP address was public and had been hacked. On the program Notepad, I was told to provide my name, email, phone number, mailing address and credit card info to get a breakdown of the charges. I was charged $110 for an Advance ID Protector, $40 for an Advance Clean Up of two computers, $50 Technician Charge and a $499 3-year web security service contract. The 1-year service contract would have cost $450…. I was told all these services were necessary to remove porn, Trojans, viruses, spyware, ransomware, hackers and be protected from future attacks…. I knew something was wrong after I tried to go to their website and got a big warning sign on my browser. Then I looked up the company on a Google Search and came across a domestic tech scam link warning about this this type of phony tech service out of Florida that was scamming people....

**OREGON**
I was working on my computer when an alarm sounded and [a] message screen popped up stating that Microsoft and Internet Explorer had errors and viruses and my computer was in danger. There was a phone number to call for support. I called the number and the person on the line, Sam, stated that I would need to log into a website... he took over...and manipulated my computer by... [uploading] software ..... He stated that for $349.99 he could protect and monitor my computer for 5 years. I paid him the money with a scanned check. Then on Oct 31 he called me back. He stated that someone tried to change my email password within the last 10 days and asked if I had. I had not. He asked to have access and I keyedi in a code and he had access. He then showed me multiple screens of errors and corruptions that were on my computer. He also informed me about safe and unsafe websites, making me feel like he really was trying to help. However, he and his software, malware, was the issue. He wanted me to pay $450.00 for lifetime protection this time. I hung up and disconnected my computer. He called me two days later and wanted to continue to discuss the issues. I told him I wanted a refund, and he refused and hung up on me.
# APPENDIX C: ADDITIONAL STORIES FROM VICTIMS

## THE VICTIMS INDEX

### #7 TECH SUPPORT SCAMS

**ALABAMA**

My father-in-law fell victim to this horrible scam last Monday. He was having issues with his computer and received a random phone call at 3 pm. The person claimed to be from Microsoft Tech Support and that he could help with his problem as long as he downloaded the proper software so Microsoft could gain access. Unfortunately, he did. The app they had him download was called Supremo. It gave them control of the computer. After this (before my father-in-law figured out what was going on), the “tech” told him that the repairs would cost $350, but that payment could only be made on iTunes gift cards. My father-in-law didn’t even know what those were, but politely refused his service (he said he felt like something wasn’t quite right). After refusing, that polite mannerism completely changed to threats. They said they were going to crash his system if he didn’t provide payment. My father-in-law hung up the phone and checked the computer. It wasn’t idle threats; they completely crashed Windows. There were multiple pop-ups with the phone number that showed up on Caller ID, and the background was completely black. I couldn’t access anything on Windows for him. His virus protection wasn’t picking it up and neither was Malwarebytes. I was able to do a complete re-installation of Windows for him, but the hackers are still calling with their threats. They have called non-stop since Monday evening (when this all began).

### #8 TRAVEL/VACATION SCAMS

**WASHINGTON**

We were approached with a vacation club membership. The company was Odyssey Premier Elite, and when we researched from our smart phones it seemed like a legitimate company. But thankfully we were still apprehensive and didn’t have a lot of money available to spend more than we did. We agreed to a total of eight weeks to be used within a five-year span for $1,750 and then an annual membership fee of $99. Odyssey Premier Elite is affiliated with a company named Blue Point Holdings LLC in Pittsburgh, Pennsylvania. After some extensive research we became suspicious so I contacted the BBB in Pittsburgh only to learn that this company does not exist there and it’s a scam. And now after researching in the BBB for Odyssey in Miami, Florida, I learned the same about this company as well. We are working with our bank to at least get the $99 annual membership fee just paid reimbursed.

**INDIANA**

I bought a timeshare with Explore Your World [for] $19,000.00 Once it was paid, there [was] no way [to] contact them. This contract was made in Mazatlan, Mexico, with representatives that Explore [Your] World company have up there. The contract [specified that] I bought 200 weeks in a period of 50 years (4 weeks per year). I paid $4000.00 as down payment. Then they offered to sell the first four [weeks] for $1000.00 each week; the balance was [to be] paid in monthly payments. Within this period of time, Angie Ramirez, customer service representative (from Miami phone number), was in contact with me and my wife. We paid this agreement in full and they gave us a user name and password but there is no way to access the system. The address in Mazatlan where we made the purchase is Avenida la Marina # 2204 Marina Mazatlan Sinaloa MX C.P. 82112 Contact Bladimir and Carlos.
#8 TRAVEL/VACATION SCAMS

**LOUISIANA**
Booked hotel room in New Orleans for Mardi Gras and paid in full six weeks in advance, through PayPal as requested. Received confirmation and payment was sent. Received an email the day before arrival stating that the hotel had overbooked but they had relocated me to another hotel, and provided another confirmation number. Personally went to the secondary hotel and showed them my confirmation; no reservation existed, none had ever been made, and the hotel personnel said they had no affiliation with the website. I immediately emailed the company—no phone number is provided to try to reach them at—and they became very defensive and threatening with each email. I was also traveling with three other parties, all of whom had booked through this company. One of them received an email that stated their rate had tripled, again they had prepaid the original rate through PayPal, and that the hotel would not honor their rate, and the other two parties went to their hotel to be told that they didn’t have rooms and had no knowledge of this company. Everyone was left without a room to stay in and for which they had already paid in full.

#9 FAMILY/FRIEND EMERGENCY SCAMS

**NORTH CAROLINA**
The caller had a northern accent. Said my father was in an accident and had hit his nephew who is involved with the Mafia and that they were holding my father until I made a payment of $2,800. He asked if my husband was there; he was, and the scammer said to move away from him, not to tell anyone or my father would be killed. I asked where he was and he said NC. I pretty much knew this as a scam after that. I was alarmed at first; then as he went on realized what was going on. When I told him I didn’t care if they shot my father (untrue) he said someone else was in the car. I asked who, and he said, “listen.” I didn’t hear anyone, and he kept assuring me that it was my mom. I told him she was in the hospital (she isn’t), and then he said it was someone else. He ….. got mad, and hung up.

**WISCONSIN**
I received a call from an Attorney (Chatow, OK, Attorney) saying that my grandson was in a DUI accident and in jail and needed money for bond. I told him I was retired and on a fixed income and that they would need to contact my son. I hung up and called my son who said my grandson was not in an accident and that he was at work.

**IDAHO**
I received a phone call from a seemingly distraught woman who claimed to be my granddaughter (actually using her name, and sounding quite a bit like her), saying she had been in an accident and was arrested. She said she was at the courthouse with her lawyer and needed $4,000 before she could go to court. My daughter, overhearing the conversation, was initially concerned about her (niece), but then, recalling scams with similar details, told me to ask the woman where the babies (her two young sons) were. She said they were fine, that they weren’t with her. My daughter was convinced it wasn’t my granddaughter on the phone. She took the phone from me and asked the woman what her mother’s name is. The woman hung up the phone. My daughter then called my granddaughter to make sure she was okay. That call confirmed the scam. Apparently, my granddaughter accepted a Friend Request on Facebook, adding me to her list. I don’t frequent Facebook at all so am unfamiliar with many of the details concerning it. My granddaughter thinks my account may have been hacked, and advised [that] I change my passwords.
# APPENDIX C: ADDITIONAL STORIES FROM VICTIMS

## THE VICTIMS INDEX

<table>
<thead>
<tr>
<th>KANSAS</th>
<th>NEW JERSEY</th>
<th>OHIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>I received a phone call from [the] government [about] grant money... He said that I qualified for [a] $7,000 grant...because I paid all my taxes on time and I’m a citizen. He told me to go to the nearest Walmart...and to call him from the parking lot for further [instructions,] and [that] this grant will be $7,300. So I went to Walmart and I bought an iTunes gift card... [for] $300. I read for him all gift card information... After that, he told me my transfer [had] been blocked. All I needed to do [was] to call another number to... [activate] my grant money, so I called...and he said I have to pay another fee to get my grant money. So I went to Walmart again and bought [another] iTunes gift card [loaded with] $800.00, and [I gave] him all the gift card information again. He said that I have to pay another fee... [and] told me to use a [MoneyGram] to send money to this person... [in] Ukraine. I said, “why Ukraine?”...he told me the transfer fee is less than [in the] USA. So I did send $1,800 to this person...He keeps telling me [about more] fees, so I find out [it] is a scam...</td>
<td>This person made a fake Facebook account using my 90-year-old grandmother’s picture and name, and messaged me to purchase a government grant. He gave me a number to contact and told me his name was Attorney Eric Holder from Washington, D.C. He told me that he is from a program created by the UN to provide federal government grants, but I had to purchase it in advance for $350. He informed me to send it through [MoneyGram] to Lisa Shelton in Pittsburgh, PA. The Caller ID states the man texting me is from Detroit. He would not let me call him, only text. He sent me a fake picture of stacked money and is now demanding my address. This cannot possibly be legal.</td>
<td>In November 2016, my house burnt down and I had no house insurance; I’m on a fixed income of Social Security. I have applied for a house grant through the CHIP Program for several months now and I have not heard a thing from them. All I want is to go home to a new place to live, where my home was burnt. So, I decided to get online and try to find another way. I have included a letter from BBB Scam [Tracker] and what happened to another lady; [and] this is [also] what happened to me. I called 202-780-9712 (Jennifer) [in] Washington DC. [She] stated I was approved for $9,200.00 for [a] government loan and stated I had to send $40.00 for [an] application fee. And then I called 646-470-9271. That person wanted me to send $800.00. Before that, I [bought] 5 gift cards total[ing] $250.00 for them, prior to them wanting me to send $800.00. Then I went to my bank and started a new account after I found out it was a scam. Are they allowed to use [the] government for these scams, and what can be done about it-[before] someone else gets taken for all their money[?]</td>
</tr>
</tbody>
</table>
Authors and Contributors

**Genie Barton** is the president of the BBB Institute for Marketplace Trust. She is something of a Renaissance woman, having begun her career as a Shakespeare scholar and first dramaturg of the Shakespeare Theatre when it was the resident troupe at the Folger Shakespeare Library. Ms. Barton then became at attorney and worked for fifteen years in the federal government, primarily in telecommunications and technology, before joining the private sector as general counsel and vice president for policy at USTelecom. As president of BBBI, she is continuing her research work in technology policy with a joint project with the Brookings Institute and the University of Michigan’s School of Information on detecting and mitigating bias in algorithmic decision-making.

**Dr. Rubens Pessanha**, senior director of market research, insights, and strategy at the Council 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 recently completed his doctorate at George Washington University. As a hobby, Dr. Pessanha teaches Project Management and Business Ethics at Strayer University.

**Melissa “Mel” Trumpower** is the director of programs and operations for the BBB Institute for Marketplace Trust. Mel has more than 20 years of experience working with not-for-profits and associations. In her last position, she created and launched a groundbreaking disaster recovery technology tool that ensures the most-needed product donations are delivered to the right place at the right time. Mel has a bachelor’s degree from Cornell University and a master’s degree from Johns Hopkins University.

**Matt Scandale** has worked for the Council of Better Business Bureaus since 1991, serving in a variety of hands-on, managerial and consulting roles in the areas of technology and data analysis, particularly in relation to operations. He specializes in development of custom database applications for internal business processes, including reporting. He hails from Buffalo, New York, and has a degree from Cornell University in consumer economics.

**Melissa Bittner** is the curriculum development and training manager with the BBB Institute for Marketplace Trust. Throughout her career, she has created educational programs, tools and experiences that bring communities together toward a common goal. Her work has supported the growth of youth programs, adult training and professional development opportunities, as well as citywide festivals and campaigns. She has a master’s degree in public administration with a concentration in ethical leadership from Marist College.

**Alexis Chng-Castor**, director of brand creative at the Council of Better Business Bureaus, is an experienced marketer and creative director with an award-winning brand portfolio. Native to Singapore and fluent in three languages, she leverages her knowledge and experience with Asian markets in all aspects of marketing and design. During her free time, she channels her love for design into her personal projects.
About the BBB Institute
The Better Business Bureau Institute for Marketplace Trust (BBB Institute) is the 501(c)(3) educational and research foundation of the Better Business Bureau. The BBB Institute educates and protects consumers; establishes best practices, guidelines and ethical standards for businesses; and leads initiatives to foster a trustworthy 21st century digital marketplace. We work with BBBs in communities across the United States and Canada to protect and empower consumers through digital and financial literacy programs, awareness campaigns and online tools. We support businesses by developing guidelines and standards for best practices and data ethics, cyber security guidelines and other digital marketplace trust issues. The BBB Institute partners with national organizations to address the latest challenges facing the digital world. Our programs include BBB Scam Tracker, AdTruth, Smart Investing, the Military & Veterans Initiative and Digital IQ.