

**2016 BBB Scam Tracker Annual Risk Report:
A New Paradigm for Understanding Scam Risk**

By Emma Fletcher | Rubens Pessanha





“This annual report highlights the insights about at-risk groups that the **BBB Scam Tracker** tool has generated. It also advances a thought-provoking new approach to risk assessment...”

BBB SCAM TRACKER [def.]: A free interactive tool for consumers in the United States and Canada to report scams and fraud while warning others of malicious activity.

FOREWORD

The Better Business Bureau Institute for Marketplace Trust (BBBI or Institute) is proud to publish the first BBB Scam Tracker Annual Risk Report. In little more than a year, BBB Scam Tracker has had a remarkable impact on the ongoing battle to prevent scams and fraud. It has educated and empowered consumers, assisted law enforcement, focused greater media attention on scams and given rise to groundbreaking research. This annual report highlights the insights about at-risk groups that the BBB Scam Tracker tool has generated. It also advances a thought-provoking new approach to risk assessment that will be of value to policymakers, enforcement agencies, consumer stakeholders and academic researchers in analyzing scams, prioritizing resource allocation and calibrating responses to scams.

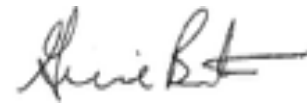
BBB Scam Tracker advances BBB's mission by protecting consumers and ethical businesses from scams that erode trust in the marketplace. Never has this been more relevant or more important. As the marketplace continues to become more complex and digital platforms grow, scammers are taking advantage of these new opportunities. They masquerade as well-respected brands, tarnishing those brands' reputations. Fraudsters cause consumers to hesitate to do business online, slowing commercial growth. Scams siphon more and more dollars from consumers and the businesses that compete fairly to earn those dollars.

BBB Scam Tracker harnesses the power of BBB to combat this growing menace. Because consumers trust BBB—the first place they think of

to report a scam—we are able to collect data from a broad base of the population, including those who were exposed to scams but were able to avoid losses. Moreover, there is a quality check on the data—each BBB reviews reports coming from consumers in their communities to weed out those that on their face do not appear to describe a scam. Because BBB is a popular source for information on scams (second only to Google when consumers are searching for information on scams) the stories reported to BBB Scam Tracker help inform the public while sending the message that this can happen to anyone. Rather than feeling like victims, those who have been scammed are energized by their ability to help prevent others from falling prey to fraudsters.

BBBI is proud to be the fulcrum for BBB Scam Tracker. This tool exemplifies the Institute's work as the catalyst for BBB innovation. BBB Scam Tracker leverages the hard work of the many dedicated women and men who make up BBB. BBBI wants to recognize their contributions and thank them. BBB Scam Tracker depends on the combined efforts of each and every BBB whose staff review and compile the consumer reports that fuel the BBB Scam Tracker tool. The BBB Scam Tracker Task Force led by BBB CEO Warren King, President of the Better Business Bureau of Western Pennsylvania, and BBBI Director of Scam and Fraud Initiatives, Emma Fletcher, guide this operation, constantly finding ways to improve the precision and effectiveness of the tool. BBBI 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 is co-author with Emma Fletcher of the seminal whitepaper, *Cracking the Invulnerability Illusion*. This study shattered common stereotypes and misconceptions about scam victimization while setting out the vision for an empowering new approach to consumer education. Together, we advance the BBB mission in new and important ways for businesses and for consumers in the 21st-century marketplace.



Genie Barton

President, Better Business Bureau
Institute for Marketplace Trust



CONTENTS

5	INTRODUCTION
6	SNAPSHOT OF 2016
7	BBB SCAM RISK INDEX <ul style="list-style-type: none">• Overview• Top 10 most risky scams
11	DEMOGRAPHICS <ul style="list-style-type: none">• Age• Gender• Geographic Area
14	SCAM DELIVERY AND PAYMENT METHODS
15	SPOTLIGHT ON MILITARY FAMILIES AND VETERANS
16	SPOTLIGHT ON STUDENTS
17	RESEARCH
18	CONCLUSION
19	APPENDIX A: Glossary of Scam Type Definitions
21	APPENDIX B: Scam Data Table
22	APPENDIX C: The Top 10 by Exposure, Susceptibility and Monetary Loss

INTRODUCTION

Marketplace scams represent a \$50 billion scourge on our economy that impacts one in four households and one in five individuals each year.¹ For more than 100 years, tackling this problem has been central to the Better Business Bureau's mission of advancing marketplace trust. BBB works to ensure that the marketplace continues to reward integrity and honesty over trickery and deceit and that the public is protected from the financial and emotional damage these crimes can leave in their wake. To maximize our efforts and those of other organizations and agencies engaged in the fight against scams, we encourage a data-driven approach, focusing limited resources where they will have the greatest impact.

With the launch of BBB Scam Tracker throughout the United States and Canada in the fall of 2015, the BBB took a giant step forward in its capacity to bring data to bear in understanding and acting on this problem. BBB Scam Tracker is a crowdsourced online tool that empowers the public to report scams and fraud and to explore reports submitted by others on an interactive "heat map." The information collected provides a window on the scam landscape, informing BBB educational efforts and outreach. Data-sharing arrangements with the Federal Trade Commission and law enforcement ensure that the information reported is available for use in criminal investigations. The data and analysis presented in this report, based entirely on reports to BBB Scam Tracker in 2016, is provided as a resource for law enforcement, policymakers, consumer advocates and educators.

In our analysis and reporting, we aim to make sense of this vast parallel marketplace, one that has similarities to legitimate commerce but is certainly far less studied and understood. Our data show that consumers accept conventional methods of payment and reach out to their targets using conventional communication methods, but the stories of those reporting to BBB Scam Tracker also tell us that they work by appealing to emotion and impulse that override the rational mind. Fraudsters may pose as trusted individuals or institutions, or they may bypass scrutiny by leveraging shared affiliation, such as a church, ethnicity or social circle. In all cases, they earn their way through deception and misappropriated trust and, in doing so, unfairly compete with honest businesses in a zero-sum game that undermines consumer confidence in a fair and ethical marketplace.

BBB Scam Tracker leverages BBB's name recognition as the number one place to turn to report a scam.² It also taps the public's desire to help. Half of those who report scams are motivated by the desire to make a difference by warning others,³ and the scams reported to BBB Scam Tracker *do* make a difference. On behalf of the more than 30,000 citizen heroes who chose to speak out and report a scam in 2016, the BBB Institute for Marketplace Trust is proud to release our first BBB Scam Tracker Annual Risk Report. It is our belief that this report will advance marketplace trust by informing ongoing efforts to protect and inform the public and business community.

Marketplace scams represent a \$50 billion scourge on our economy that impacts



one in four households and



one in five individuals each year.

NOTE

¹ Martha Deevy and Michaela Beals. *The Scope of the Problem: An Overview of Fraud Prevalence Measurement*. Financial Fraud Research Center, 2013. http://fraudresearchcenter.org/wp-content/uploads/2013/11/Scope-of-the-Problem-FINAL_corrected2.pdf

² Emma Fletcher and Rubens Pessanha. *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*. BBB Institute for Marketplace Trust, 2016. www.bbb.org/truthaboutscams

³ Ibid.

SNAPSHOT OF 2016

In 2016, more than 32,000 reports were submitted to BBB Scam Tracker, an average of about one report every 15 minutes (Table 1). These reports were received from individuals in the United States and Canada, representing a cross-section of the population. Reports were classified into 30 scam types (Appendix A) as well as an “other” category representing 5.8% of all reports. Data collected

included a description of the scam, the dollar value of any loss, information on 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 and student status. See Appendix B for more detailed data by scam type.

Table 1: Snapshot of 2016

Total Number of BBB Scam Tracker Reports	32,781
% Susceptibility (i.e., % of reports that included \$ Loss)	18.8%
Median Dollar Loss ⁴	\$274
Top Means of Contact	Phone
Top Method of Payment	Credit Card



< 30 Different Types of Scams

NOTE

⁴ All dollar values in this report have been converted to USD except where otherwise noted.

BBB SCAM RISK INDEX

OVERVIEW

Past attempts to compare scam types by relative risk have generally consisted of simple rankings by frequency of exposure. This volume-based approach fails to acknowledge the multifaceted nature of scam risk. In fact, 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, as we have done with the BBB Risk Index (Figure 1), we are able to gain a far more meaningful measure of the relative risk of a given scam type.⁵ This information can be a driver for focusing educational and investigative efforts where they are likely to have the greatest effect. This analysis also can be used to understand how risk varies by geographic region and by particular subgroups of the population, such as military personnel, 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 e-mail or robocall 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 even greater concern if median losses are extremely high. The Index captures these real-world elements by representing the intersection of exposure, susceptibility and monetary loss.

We believe the Index represents a major advance in our ability to take a data-driven approach to combatting marketplace scams. It effectively distills the elements of risk we are able to glean from crowdsourced reporting into a single measure that is as powerful as it is simple to grasp and apply, both on a national scale and in parsing the data to explore differences in risk borne by particular subsets of the population. We encourage others, including academics, law enforcement, consumer advocates and policymakers, to consider how best to calibrate this information in the context of what they are trying to achieve. We welcome ongoing discussion, collaboration and further study on the topic of risk as it relates to scams as well as the interplay of risk with other factors—such as median household income—that may make the financial harm caused by scams more or less burdensome to a particular population.

BBB SCAM 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.

NOTE

⁵ 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 reflection of the true nature of the problem. BBB reviews reports to determine if they describe what a reasonable person would believe to be a scam, but does not validate all 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 in the Index.

Figure 1: BBB Risk Index Formula



The formula for calculating the BBB Scam Risk Index for a given scam type in a given population is Exposure X Susceptibility X Median Loss/Overall Median Loss X 1,000. Median loss for the scam type is divided by the overall median dollar amount of all losses reported to control for currency fluctuations, ensuring that results can be compared over time and across currencies. As a final step, the result was multiplied by 1,000 to clear decimals.

TOP 10 MOST RISKY SCAMS

Table 2 reflects the top 10 most risky scam types based on all reports to BBB Scam Tracker in 2016 (United States and Canada combined) and was calculated by applying the BBB Scam Risk Index formula. This ranking

provides our best measure of the relative risk of the scam. The BBB Scam Risk Index score enables ranking of scam types by relative risk, and also reflects the relative magnitude of the risk (e.g., employment scams are approximately twice as “risky” as tech support scams by

this measurement method). Appendix C provides top 10 rankings for each of the three Risk Index elements. As discussed earlier, each of these elements taken alone provides an incomplete picture of relative risk.

Table 2: Top 10 Scams by BBB Risk Index

#	Scam Type	BBB Scam Risk Index	% Exposure	Susceptibility %	Median Loss \$	Most Susceptible ⁶	Primary Contact & Payment Method
1	Home Improvement	26.8	1.0%	53.4%	\$1,400	Males age 55-64	In-Person Check
2	Fake Check/Money Order	25.9	3.1%	15.8%	\$1,471	Males age 18-24	E-mail Check
3	Employment	25.8	6.3%	16.7%	\$671	Males age 25-34	E-mail Check
4	Online Purchase	23.0	8.4%	74.1%	\$101	Females age 18-24	Website Credit Card
5	Advance Fee Loan	22.4	3.3%	36.4%	\$510	Males age 18-24	Phone Wire Transfer
6	Investment	19.8	0.6%	51.0%	\$1,800	Males age 55-64	Phone Wire Transfer
7	Romance	13.0	0.3%	48.5%	\$2,373	Males age 45-54	Website Wire Transfer
8	Tech Support	12.0	4.8%	22.9%	\$299	Females age 18-24	Phone Credit Card
9	Family/Friend Emergency	11.2	0.8%	18.8%	\$2,174	Males age 65+	Phone Wire Transfer
10	Sweepstakes/Lottery/Prizes	11.1	7.3%	8.4%	\$500	Females age 18-24	Phone Wire Transfer

NOTE

⁶ Represents the demographic group most likely to lose money when exposed to the scam type. Demographic groups with fewer than 30 reports for a given scam type were excluded.

SELECTED VICTIM **STORIES**

HOME IMPROVEMENT SCAM

"Owner of company was driving in my neighborhood looking at driveways needing sealcoating. Asked if he could do ours. Gave us one of his business fliers. Twenty-four hours later, after rains, half of sealcoating washed away. Cracks were not filled. We made multiple attempts to contact owner to return and repair. Owner never came back to repair."

FAKE CHECK/MONEY ORDER SCAM

"I was e-mailed instructions to accept a check that would cover travel arrangements and deposit the check and then wire money to a 'travel agent' account. I deposited the money into the account and two days later the original check I sent has bounced and now I owe the bank."

EMPLOYMENT SCAM

"I was looking for work that I could do from home and after listening to the company and all its potential I invested \$17,000. The company has delivered nothing."

ONLINE PURCHASE SCAM

"Buying a motorcycle off Craigslist. The seller asked if it was okay to do the transaction through Google Wallet. We agreed. They said we had to buy gift cards and load them with the amount of the purchase onto iTunes gift cards. Now we are out a lot of money."

ADVANCE FEE LOAN SCAM

"I really needed to pay this bill last week, so I contacted the man after I read the e-mail he sent me. He told me I would get the loan of \$1,500 by MoneyGram and I needed to send \$70 to pay the fees, so I did. The next day he told me I needed to pay \$100 for insurance on the loan, so I did. The next day, he came up with another fee I needed to pay, and I did not get the loan."

INVESTMENT SCAM

"Requires you make a \$500 deposit and in 10 days your money will increase 18%. I see my money growing as they say it will daily, but when I request a withdrawal it's been pending for weeks."



SELECTED VICTIM **STORIES**

ROMANCE SCAM

"We started sending messages to each other through the site. Supposedly, he was a soldier deployed in Kabul, Afghanistan. We grew to love each other (I later realized it was all fake). I shared personal information about my family. Everything was going so well, supposedly, that he decided he was going to request a leave to come and meet with me and my children. That is when he started asking me for money."

TECH SCAM

"They set up a warning that looked like it came from Microsoft saying that the safety of my IP address had been compromised and that my computer had been hacked and was about to crash. The warning said I had to call a number to get the issue solved, and the warning would not go away, so my computer was frozen on that screen. I called the number and was given no option but to proceed to pay them \$500 to 'fix' the 'problem.' "

FAMILY/FRIEND EMERGENCY SCAM

"Person called as my nephew that he had been in a car wreck in Mexico City, Mexico and noted that they had put him in a holding cell. Stated they took his passport and would not be released unless just under \$1,000 in fines and court cost was paid. Gave the phone to his so-called lawyer who said he was a lawyer from the US Embassy. Person sounded like my nephew and knew family information. I wired exact amount by Western Union. Not hearing from my nephew, I called him today and he was in Ontario, Canada . . . knew nothing about the scam."

SWEEPSTAKES/LOTTERY/PRIZES SCAM

"I was contacted by phone and was told I had won the second prize in the Publisher's Clearing House. My prize was supposed to be a cashier's check in the amount of \$950,000 and a Mercedes automobile. However, I was told there were certain taxes and fees that needed to be paid up front before I could receive my delivery. Over several months, I sent them various amounts using various methods such as MoneyGram, Western Union and money orders."



DEMOGRAPHICS

The collection of self-reported demographic data such as age, gender and 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 40% of individuals who provided age information when reporting to BBB Scam Tracker were over the age of 55, 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 targeted by, or may be related to differences in access to financial resources with increasing age.

One important caveat with respect to age-related findings is that seniors experiencing cognitive impairment are likely more vulnerable to scams and abuse by caretakers, including financial abuse, but may be less likely to report their experiences to BBB Scam Tracker.

In targeting prevention efforts by age group, it may be beneficial to understand the types of scams that each group is most at risk from. The BBB Risk Index formula has been calculated for each age group to identify the top three most risky scams (see Table 3).

Figure 2: Susceptibility and Median Loss by Age

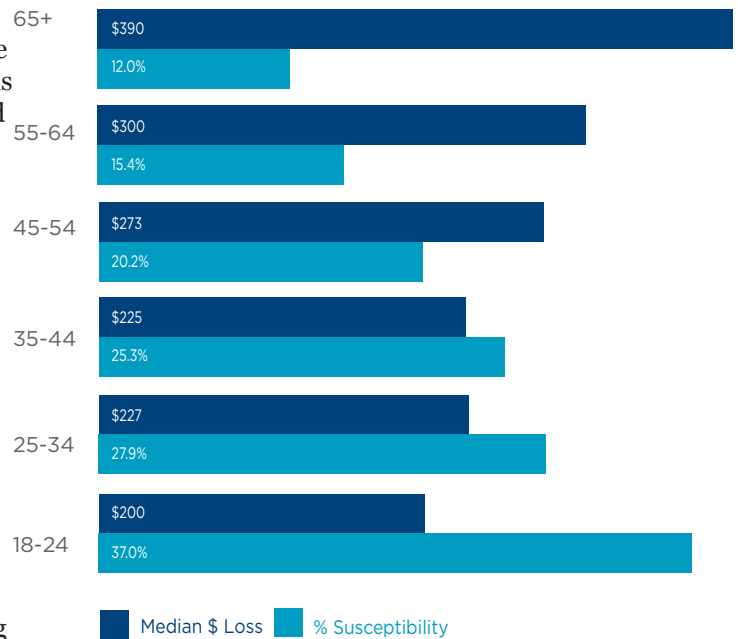


Table 3: Top 3 Scams by Age Range

AGE RANGE	TOP 3 MOST RISKY SCAM TYPES*		
	1	2	3
18-24	Fake Check/Money Order	Online Purchase	Employment
25-34	Employment	Fake Check/Money Order	Online Purchase
35-44	Investment	Home Improvement	Advance Fee Loan
45-54	Home Improvement	Advance Fee Loan	Phishing
55-64	Home Improvement	Travel/Vacations	Fake Check/Money Order
65+	Family/Friend Emergency	Sweepstakes/Lottery/Prizes	Travel/Vacations

*Excluded scam types with less than 30 reports for the specified group.

GENDER

Overall, women were nearly twice as likely to report a scam to BBB Scam Tracker as men. However, this increased tendency to report is not necessarily an indicator of greater frequency of victimization or greater losses. Women appear to be slightly less susceptible to loss when exposed to a scam (Figure 3). Median dollar losses for women are also substantially lower than for men (Figure 3). 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 4).

Figure 3: Susceptibility and Median Loss by Gender



Table 4: Top 3 Scams by Gender

AGE RANGE	TOP 3 MOST RISKY SCAM TYPES		
	1	2	3
Females	Online Purchase	Home Improvement	Fake Check/ Money Order
Males	Investment	Home Improvement	Advance Fee Loan

GEOGRAPHIC AREA

Median loss and the riskiest scams show some variability by region. 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 marketplace and demographic differences by region that in turn correlate with differing levels of exposure 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.

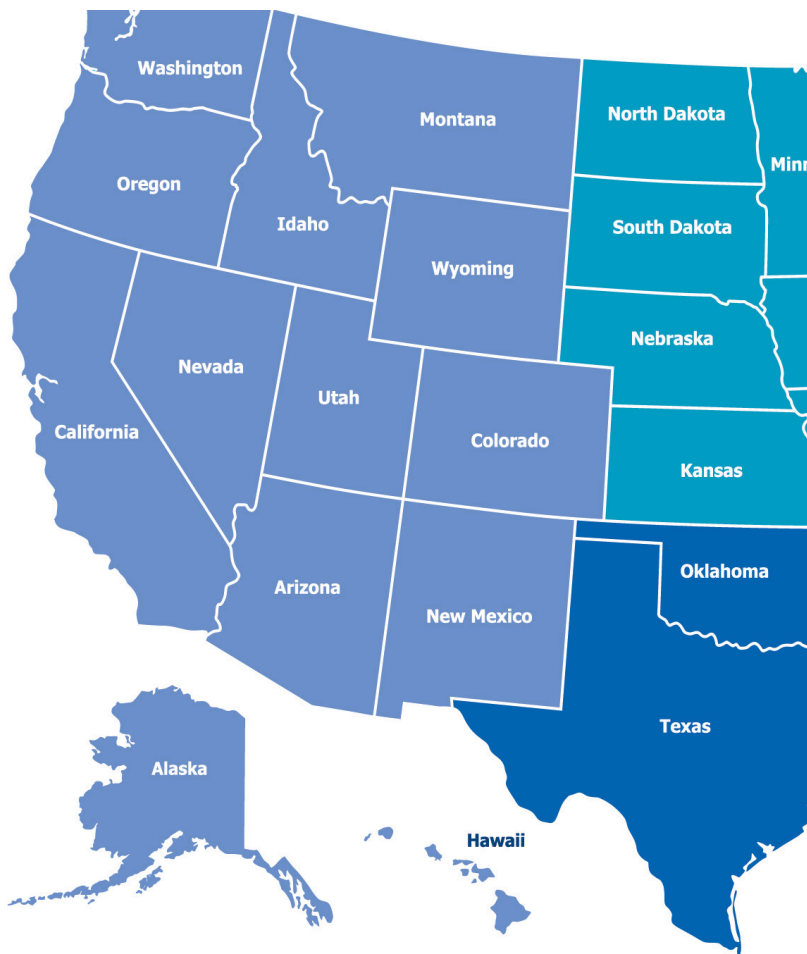




Figure 4: Most Risky Scam Types by Geographic Area

Canada Region	Median CAD Loss	Most Risky Scam [^]
Eastern	\$370	Advance Fee Loan
Western and Northern	\$300	Advance Fee Loan
Total Number of Reports in Canada = 1,520 (4.6% of total reports)		

US Region	Median USD Loss	Most Risky Scam [^]
Midwest	\$231	Employment
Northeast	\$228	Online Purchases
South	\$300	Home Improvement
West	\$299	Investment
Total Number of Reports in the US = 31,261 (95.4% of total reports)		

[^]Excluded scam types with fewer than 30 reports for the specific region.

SCAM DELIVERY AND PAYMENT METHODS

Fraudsters exploit the full range of communication channels to make contact with their targets and readily adapt to incorporate new communication methods or popular mediums. Figure 5 provides a comparison of all scam delivery methods reported to BBB Scam Tracker in 2016 where a monetary loss occurred. Scams delivered by phone were the most frequently reported. However, the combined total of the various forms of online scam delivery (i.e., e-mail, website, social media, online classifieds, Internet messaging) accounts for more than half of all reports of monetary loss.

The range of payment methods used by scammers (Figure 6) is consistent with the variability and adaptability seen generally 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 considered a red flag for fraud.

Figure 5: Means of Contact

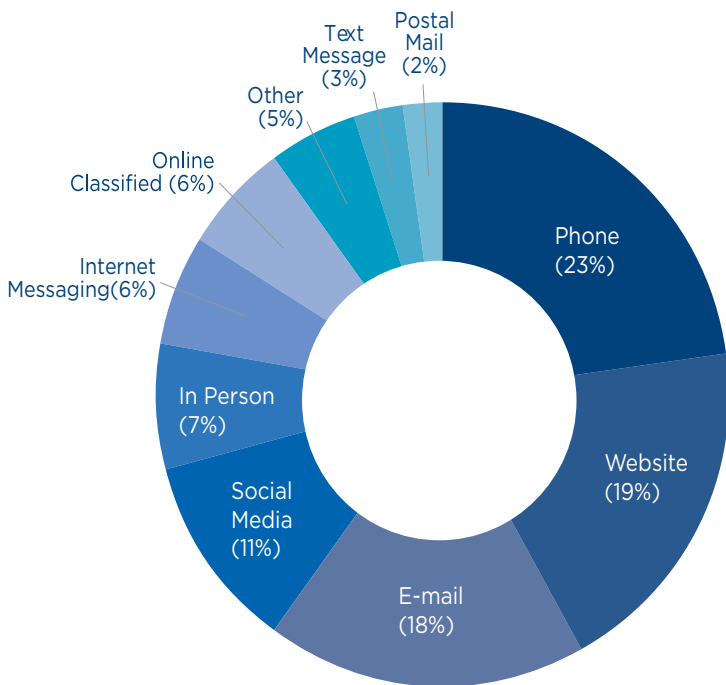
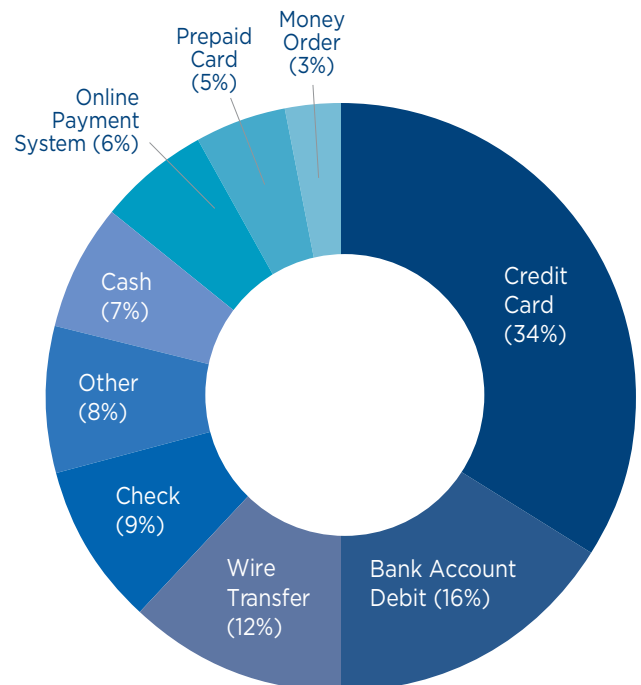


Figure 6: Payment Methods



SPOTLIGHT ON MILITARY FAMILIES AND VETERANS

Military families and veterans have long been recognized as being 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 8.5% of reports to BBB Scam Tracker.⁷ These individuals may be more susceptible when exposed to a scam, with 21.0% reporting losses compared to 18.6% of non-military individuals. More striking is the median loss of \$350, nearly 35% higher than the non-military median loss of \$260. The BBB Risk Index formula has been applied to identify the top three riskiest scams for military families and veterans.

Figure 7: Susceptibility and Median Loss by Military Families and Veterans

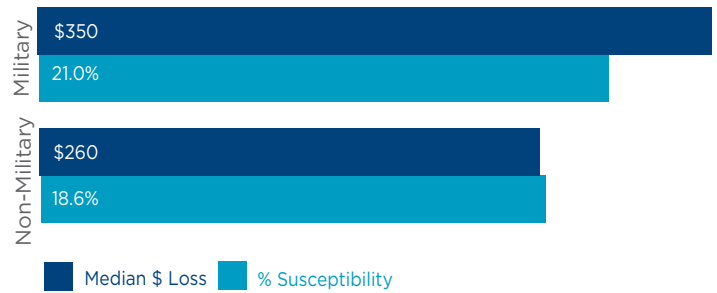


Table 5: Top 3 Scams by Military Families and Veterans

Military Target	TOP 3 MOST RISKY SCAM TYPES [#]		
	1	2	3
	Fake Check/Money Order	Travel/Vacations	Tax Collection

[#]Excluded scam types with fewer than 30 reports.

NOTE

⁷ 8.5% of reports since February 5, 2016 were from individuals who identified as “active duty military, veteran, or spouse.” Prior to that date, this information was not collected.

SPOTLIGHT ON STUDENTS

Individuals who self-identified as students represent 7.1% of reports to BBB Scam Tracker. These individuals appear to be significantly more vulnerable when exposed to a scam as 32.4% of students reported a loss as compared to 17.7% of reports from non-students (Figure 8). However, the median dollar loss of \$200 for this group is significantly lower than the median loss for non-students of \$296 (Figure 8). This may reflect differences in the scam types students are most vulnerable to as well as differences in access to funds. It should also be noted that the susceptibility rate and median losses for students are very similar to those of the 18-24 age category that includes most students.

Figure 8: Susceptibility and Median Loss for Students

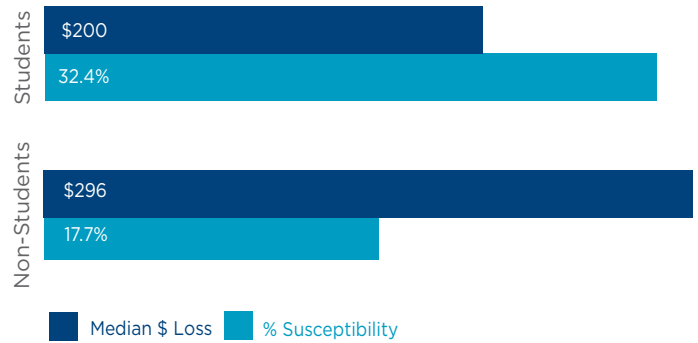
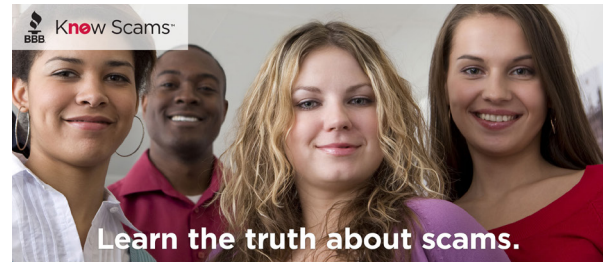
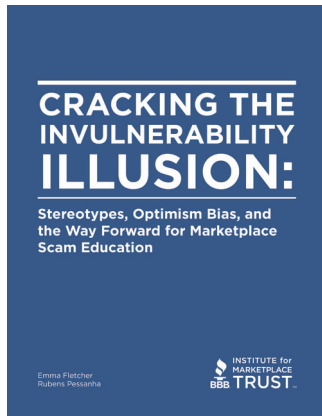


Table 6: Top 3 Scams for Students

Student Target	TOP 3 MOST RISKY SCAM TYPES		
	1	2	3
	Fake Check/Money Order	Employment	Online Purchase

RESEARCH



Receive your free copy of our research study today.

CRACKING THE INVULNERABILITY ILLUSION

Download Now

Marketplace Scams Affect One in Four Households Annually

The estimated loss to individuals and families of \$50 billion each year, yet most consumers believe it can't happen to them. In 2016, the Better Business Bureau surveyed consumers in the U.S. and Canada to try to understand why. We hope our paper will dispel common misperceptions, and point to a new direction for consumer education and awareness efforts aimed at preventing scam victimization.

<p>Stereotypes about scam victims stand in sharp contrast with reality. The public believes victims are likely to be elderly or ignorant. In fact, we are all at risk.</p>	<p>Helping to warn others is a key motivator for reporting scams. Underreporting has been a long-standing challenge to law enforcement investigations and public education.</p>	<p>Recognizing a scam isn't always easy, but knowing what to look for in advance is key to scam avoidance.</p>
---	--	---

Learn the 5 myths about scams.

[Click to view infographic.](#)

INSTITUTE for MARKETPLACE BBB TRUST™

We thank the thousands of individuals who have come forward to help warn others by reporting scams to BBB Scam Tracker. We would also like to recognize the extraordinary contribution of FINRA Investor Education Foundation, the Federal Trade Commission, the National Cyber Security Alliance and APWG in advancing research and education in this space, as well as countless corporations that have contributed their ingenuity to create fraud-prevention solutions.

In 2016, BBBI published a primary research paper utilizing BBB Scam Tracker data as well as survey research data. This paper, *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias and the Way Forward for Marketplace Scam Education*, offered key findings and recommendations based on a BBBI 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 of scam victims, and 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 the hope of recovering lost funds or bringing the perpetrator to justice.
- U.S. respondents identified BBB as the number one resource for reporting scams and second only to Google for researching scams.

For more information or to download this whitepaper, visit bbb.org/TruthAboutScams.



CONCLUSION

“Together, we can and do make a difference in the fight against marketplace scams.”

This report is an important milestone in the use of BBB Scam Tracker data to inform a larger collaborative effort to combat marketplace scams. Consumers and ethical businesses rely on the marketplace to operate by a playbook where fair and honest practices are rewarded. Scammers break these rules, unfairly gaining the upper hand. It is our hope that this report will be applied as a tool to inform decisions in education and enforcement and, in doing so, encourage an approach to this problem that tips the scales ever more decisively in favor of marketplace trust and honest and ethical business practices.

We thank the thousands of individuals who made this report possible by reporting scams to BBB Scam Tracker. Please continue to learn about and report scams at bbb.org/scamtracker. Your efforts help others to avoid scams and advance our collective knowledge and understanding of this problem. We would also like to recognize the contribution of the Federal Trade Commission, FINRA Investor Education Foundation and the Stanford Center on Longevity in advancing research and education in this space, as well as countless corporations that have contributed their ingenuity to create fraud-prevention solutions. Together, we can and do make a difference in the fight against marketplace scams.

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 classifications used by the Federal Trade Commission and the Internet Crime Complaint Center of the FBI. While scams vary widely, nearly 95% of all scams reported to BBB Scam Tracker can be classified into one of these general types.

Scam Types	Definitions
Advance Fee Loan Scams	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.
Business E-mail Compromise	This financial fraud targets businesses engaged in international commerce. Scammers gain access to company e-mail and trick employees into sending money to a “supplier” or “business partner” overseas.
Charity Scams	Charity scams use deception to get money from individuals who believe they are making donations to legitimate charities. This is particularly common in the wake of a natural disaster or other tragedy.
Counterfeit Products	Counterfeit goods mimic original merchandise, right down to the trademarked logo, but are typically of inferior quality. This can be a life-threatening health or safety hazard when the counterfeit item is medication or an auto part.
Credit Card Scams	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.
Credit Repair/ Debt Relief Scams	Scammers posing as legitimate services collect payment in advance with promises of debt relief and repaired credit but provide little or nothing in return.
Debt Collection Scams	In this con, phony debt collectors harass their targets, trying to get them to pay debts they don’t owe.
Employment Scams	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.
Fake Checks and Money Orders	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.
Fake Invoice Scams	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.
Family/Friend Emergency Scams	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 provided on social media, imposters can offer very plausible stories to convince their targets.
Government Grant Scams	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.
Health Care, Medicaid and Medicare Scams	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.
Home Improvement Scams	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.
Identity Theft	Identity thieves use personal information (e.g., Social Security numbers, bank account information and credit card numbers) to pose as another individual. This may include opening a credit account, draining an existing account, filing tax returns or obtaining medical coverage.
Investment Scams	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.
Moving Scams	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.
Foreign Money Exchange Scams	In this scam, the target receives an e-mail 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.

Scam Types	Definitions
Online Purchase Scams	These cons involve purchases and sales, often on eBay, Craigslist, Kijiji or other direct seller-to-buyer sites. Scammers may pretend to purchase an item only to send a bogus check and ask for a refund of the “accidental” overpayment. In other cases, the scammer will simply never deliver the goods.
Phishing	Communication impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information or passwords.
Rental Scams	Phony ads for rental properties ask for advanced payments. Victims later discover the property doesn’t exist or is owned by someone else.
Romance Scams	An individual believing they are in a romantic relationship is tricked into sending money, personal and financial information or items of value to the perpetrator.
Scholarship Scams	This con hooks victims, often students struggling with tuition costs, with the promise of government scholarship money, but upfront “fees” never actually materialize into 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.
Malware	Any kind of computer bug with malicious intent. One type of malware, called “spyware,” is designed to steal personal information. “Adware” displays unwanted ads. “Ransomware” can hold data on a device hostage until the scammer is paid to unlock it.
Sweepstakes, Lottery and Prize Scams	This con fools victims into thinking they have won a prize or lottery jackpot, but need to pay upfront fees to receive the winnings, which never materialize. Sometimes this con involves a fake check and a request to return a portion of the funds to cover fees.
Tax Collection Scams	In this con, imposters posing as an Internal Revenue Service representative in the United States or as the Canada Revenue Agency in Canada attempt to coerce the target into either paying up or sharing personal information. Threats of immediate arrest and other scare tactics are common.
Tech Support Scams	Tech support scams start with a call or pop-up warning alerting the target to a computer bug or other problem. Scammers pose as tech support employees of well-known computer companies and hassle victims into paying for “support.” If the victim allows remote access, malware may be installed.
Travel and Vacation Scams	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.
Utility Scams	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.
Yellow Pages/Directory Scams	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.

APPENDIX B: SCAM DATA TABLE

Scam Types	Count	%Exposure	%Susceptibility	Median \$ Loss	Risk Index	Top Mean of Contact	Top Payment Method
Advance Fee Loan Scams	1,085	3.3%	36.4%	\$510	22.4	Phone	Wire Transfer
Business E-mail Compromise	127	0.4%	26.0%	\$200	0.7	E-mail	Credit Card
Charity Scams	240	0.7%	17.9%	\$130	0.6	Phone	Check
Counterfeit Products	463	1.4%	53.1%	\$150	4.1	Phone	Credit Card
Credit Card Scams	904	2.8%	22.1%	\$158	3.5	Phone	Credit Card
Credit Repair/ Debt Relief Scams	487	1.5%	23.2%	\$599	7.6	Phone	Bank Account Debit
Debt Collection Scams	2,798	8.5%	6.8%	\$437	9.2	Phone	Bank Account Debit
Employment Scams	2,066	6.3%	16.7%	\$671	25.8	E-mail	Check
Fake Checks and Money Orders	1,000	3.1%	15.8%	\$1,471	25.9	E-mail	Check
Fake Invoice Scams	812	2.5%	12.1%	\$313	3.4	Postal Mail	Check
Family/Friend Emergency Scams	245	0.8%	18.8%	\$2,174	11.2	Phone	Wire Transfer
Government Grant Scams	1,587	4.8%	9.6%	\$650	11.1	Phone	Prepaid Card
Health Care, Medicaid and Medicare Scams	218	0.7%	11.0%	\$325	0.9	Phone	Credit Card
Home Improvement Scams	322	1.0%	53.4%	\$1,400	26.8	In Person	Check
Identity Theft	355	1.1%	12.4%	\$200	1.0	Phone	Credit Card
Investment Scams	192	0.6%	51.0%	\$1,800	19.8	Phone	Wire Transfer
Moving Scams	56	0.2%	76.8%	\$250	1.2	Phone	Cash
Foreign Money Exchange Scams	176	0.5%	12.5%	\$1,100	2.7	E-mail	Wire Transfer
Online Purchase Scams	2,763	8.4%	74.1%	\$101	23.0	Website	Credit Card
Phishing	1,249	3.8%	5.8%	\$400	3.2	Phone	Credit Card
Rental Scams	349	1.1%	40.1%	\$350	5.4	Online Classifieds	Cash
Romance Scams	101	0.3%	48.5%	\$2,373	13.0	Website	Wire Transfer
Scholarship Scams	39	0.1%	20.5%	\$105	0.1	Phone	Credit Card
Malware	469	1.4%	31.3%	\$300	4.9	Phone	Credit Card
Sweepstakes, Lottery and Prize Scams	2,383	7.3%	8.4%	\$500	11.1	Phone	Wire Transfer
Tax Collection Scams	7,902	24.1%	0.9%	\$1,000	7.9	Phone	Prepaid Card
Tech Support Scams	1,580	4.8%	22.9%	\$299	12.0	Phone	Credit Card
Travel and Vacation Scams	303	0.9%	38.0%	\$847	10.8	Phone	Credit Card
Utility Scams	286	0.9%	6.6%	\$500	1.1	Phone	Prepaid Card
Yellow Pages/Directory Scams	340	1.0%	7.4%	\$500	1.4	Fax	Credit Card
Other	1,884	5.8%	25.4%	\$400	21.3	Phone	Credit Card
Total	32,781	100%	18.8%	\$274	NA	NA	NA

APPENDIX C: TOP 10 BY EXPOSURE, SUSCEPTIBILITY, AND MONETARY LOSS



Top 10 By

Exposure

1 Tax Collection Scams	2 Debt Collection Scams	3 Online Purchase Scams	4 Sweepstakes, Lottery and Prize Scams	5 Employment Scams
6 Government Grant Scams	7 Tech Support Scams	8 Phishing Scams	9 Advance Fee Loan Scams	10 Fake Check/ Money Order Scams

Susceptibility

1 Moving Scams	2 Online Purchase Scams	3 Home Improvement Scams	4 Counterfeit Products	5 Investment Scams
6 Romance Scams	7 Rental Scams	8 Travel & Vacation Scams	9 Advance Fee Loan Scams	10 Malware

Median \$ Loss

1 Romance Scams	2 Family & Friend Emergency Scams	3 Investment Scams	4 Fake Check/ Money Order Scams	5 Home Improvement Scams
6 Foreign Money Exchange Scams	7 Tax Collection Scams	8 Travel & Vacation Scams	9 Employment Scams	10 Government Grant Scams

About the Authors

Emma Fletcher is the director of scam and fraud initiatives with the BBB Institute for Marketplace Trust, the educational foundation of the Council of Better Business Bureaus. She has more than two decades of experience in dispute resolution and consumer protection, particularly in the areas of marketplace scams, identity theft and privacy. She is a Certified Information Privacy Professional and holds a master's degree in public administration from George Mason University.

Rubens Pessanha, director of market research and insights with 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 the United States, Japan, South Africa, Belgium and his native Brazil. A production engineer with an MBA, he is about to finish his doctorate at George Washington University.

The BBB Institute for Marketplace Trust is the educational foundation of the Council of Better Business Bureaus and a nonprofit 501(c)(3) organization. Its goal is to connect targeted consumer populations to BBB services, promote consumer awareness and financial literacy and advance business ethics in the marketplace. The organization offers in-person training, print and digital educational resources, scholarships and recognition programs that promote ethical enterprise and fraud prevention across North America.

