

Tech-Savvy Scammers Work to Con More Victims

*2018 BBB
Scam Tracker
Risk Report*





Table of Contents

4	Introduction
5	- About BBB Scam Tracker SM
6	Snapshot of 2018
10	BBB Risk Index: A Three-Dimensional Approach to Measuring Scam Risk
12	- 10 Riskiest Scams
18	Demographics
18	- Age
20	- Gender
22	- Geographic Area
23	Scam Delivery and Payment Methods
28	Spotlight on Military Families and Veterans
30	Spotlight on Students
32	Spotlight on Impersonated Organizations
34	<u>KNOW</u> Scams
34	- 10 Tips for Avoiding a Scam
35	Conclusion
35	- About BBB Institute
36	BBB Research
38	Appendix A: Glossary of Scam Type Definitions
40	Appendix B: Scam Data Table
41	Appendix C: Top 10 Scam Types by Overall Risk, Exposure, Susceptibility, and Monetary Loss




Introduction

The BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the Better Business Bureau (BBB), is pleased to present *Tech-Savvy Scammers Work to Con More Victims: 2018 BBB Scam Tracker Risk Report*. This report is produced each year using timely data submitted by consumers to BBB Scam TrackerSM ([BBB.org/ScamTracker](https://www.bbb.org/ScamTracker)) to shed light on how scams are being perpetrated, who is being targeted, which scams have the greatest impact, and much more. Key highlights are provided in Figure 1.

In 2018, according to BBB Scam Tracker data, the number of scams reported continued to climb. Each year, scams rob consumers and legitimate businesses of billions of dollars, and thus erode consumer confidence in the marketplace. Insights in the *2018 BBB Scam Tracker Risk Report* help to provide a clearer picture of the impact scams have on consumers and businesses as well as specific cohorts. BBB works with officials in business, law enforcement, government, and the not-for-profit sector to determine the best ways to reduce the impact of scammers.

The inaugural *2016 BBB Scam Tracker Risk Report* introduced the BBB Risk Index (Figure 2), a multidimensional approach to evaluating scam risk. By considering three dimensions—exposure, susceptibility, and monetary loss—we are able to provide a more meaningful measure of the relative risk of a given scam type. Information submitted to BBB Scam Tracker enables us to parse the data to explore differences in risk borne by particular subsets of the population and provide useful insights regarding messaging to educate consumers about how to avoid falling prey to scams.

Findings provided in this year's report are used to support and inform BBB Institute's educational programs, which aim to inform and empower consumers and legitimate businesses. Our consumer education efforts are critical to limiting the financial and emotional



damage to victims as well as restoring consumer confidence in honest businesses so the marketplace can flourish. A healthy marketplace requires empowered and aware consumers and principled businesses that are proactively working to stop scammers.

We believe the insights provided by the *2018 BBB Scam Tracker Risk Report* will advance marketplace trust by providing an in-depth look at the 2018 scam landscape and enabling us to develop new strategies to grow awareness about the tactics used by scammers.

This report would not be possible without 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. We extend our thanks to the 150,000 citizen heroes who chose to speak out by reporting scams since the launch of BBB Scam Tracker in 2015.



About BBB Scam TrackerSM

Data in the *2018 BBB Scam Tracker Risk Report* is provided via BBB Scam Tracker, an online tool that enables consumers and businesses to report scams to BBB in an effort to prevent others from falling prey to similar cons. By using technology to collect scam reports from consumers and businesses, and utilizing the power of our network of Better Business Bureaus working in communities across the United States and Canada, BBB Scam Tracker maximizes our efforts to educate consumers and stop fraudsters.

The scam reports submitted to BBB Scam Tracker are made available to the general public via an interactive website. The website features a searchable “heat map” that enables users to view the number and types of scams reported in their communities. This allows consumers and businesses to take action by sharing their knowledge and reporting scams they’ve encountered. By working together, we can all fight back against scammers who steal billions and erode marketplace trust.

Snapshot of 2018

In 2018, more than 50,000 scam reports were published via BBB Scam Tracker, representing a steady increase in reported scams since the website was launched in 2015. These reports were received from businesses and individuals across North America, representing a cross-section of the population. Reports were classified into 30 scam types (Appendix A), plus an “other” category that represented 4.7 percent of all reports. Data collected included a description of the scam, the dollar value of any loss,¹ and information about the means of contact and method of payment. Optional demographic data—age, gender, and postal code—of the victim or target were also collected, along with military and/or student status. See Appendix B for more detailed data by scam type.

In 2018, scams reported to BBB Scam Tracker rose almost 6 percent, from 47,827 reports in 2017 to 50,559 scam reports in 2018; the previous rise in reports from 2016 to 2017 was approximately 46 percent.²

The overall median dollar loss fell 33.3 percent, from \$228 in 2017 to \$152 in 2018. This decrease continued the drop we reported in the 2017 report, which had fallen from a median dollar loss of \$274 in 2016 (Table 1). This decrease could be connected to the large number of online purchase scams reported in 2018, which tend to result in a lower median dollar loss; the median dollar loss for online purchase scams in 2018 was \$75.



In 2018, more than 50,000 scam reports were published via BBB Scam Tracker, representing a steady increase in reported scams since the website was launched in 2015.

Although the median dollar loss dropped again in 2018, consumers lost money more often when exposed to a scam. In fact, susceptibility (the percentage of consumers who lost money when exposed to a scam) increased 86.7 percent in 2018 to 29.5 percent, up from 15.8 percent in 2017 (Table 1). This sharp increase may, in part, also be related to the huge increase in online purchase scams, which made up 20.6 percent of all scams reported to BBB Scam Tracker, up from 9.7 percent in 2017. In 2018, when consumers who reported to BBB

¹ All dollar values in this report have been converted to USD.

² In 2017, 10,670 “Can You Hear Me Now” scams were reported, significantly increasing reported scams from 2016 to 2017. Because none of those scams resulted in a monetary loss, we are not sure this was an actual scam. If we correct for that bump (removing the 10,670 reports from the 2017 total), we see that the increase from 2017 to 2018 was closer to an increase of about 36 percent (from 37,157 scams in 2017).

Scam Tracker were exposed to online purchase scams, they lost money 75.2 percent of the time. This is extremely high when compared to the overall susceptibility of 29.5 percent.

Technology continued to be exploited by scammers in 2018. The increase in online purchase scams was likely because more people are conducting business (personal and professional) online. Phones were the top means of contact overall for the third year in a row; however, 2018 was the first time websites eclipsed phones as the top means of contact for scams reporting a monetary loss. Also notable this year, scams perpetrated through social media with a monetary loss increased from 13 percent in 2017 to 20 percent in 2018. Email remained a common mode of contact, with fraudsters spoofing legitimate businesses. When the most popular means of contact for all scams are compared with the means of contact resulting in a monetary loss, it appears people are more likely to lose money when they are contacted online (including via website or social media) in comparison to by phone. This indicates more education should be focused on those areas.

In 2018, we added a new scam category to account for reports involving cryptocurrencies. Many of the BBB Scam Tracker reports regarding cryptocurrency fraud were submitted as investment scams.³ We also added cryptocurrency as a payment type (a breakout of payment types used by scammers is available in Figure 7).

Additional insights provided in the full report offer greater detail about specific scam types and break those types out by demographics to show which cohorts are most vulnerable to certain types of scams. We encourage you to dig deeper into the data and insights provided here. We believe more must be done to prepare the average consumer to ensure they do not fall prey to scammers. The *2018 BBB Scam Tracker Risk Report* is one piece of a larger, multifaceted consumer education effort.

³ We added the new cryptocurrency scam category in August and manually adjusted the investment and cryptocurrency scam types by searching the text fields to classify them into the correct category.

FIGURE 1

KEY RISK REPORT HIGHLIGHTS

THE Riskiest 5 Scams

1 EMPLOYMENT

A job offer comes with high pay and options to work remotely and with flexible hours. To get the job, a candidate must complete forms that require personal, sensitive information and may be required to “purchase equipment” with part of the proceeds of what turns out to be a fake check.

2 ONLINE PURCHASE

A buyer makes a purchase online from an individual seller or company, but the item never arrives. Or in other cases, a person sells an item online, but the check received for payment is fake.

3 FAKE CHECK/MONEY ORDER

A check is sent to a consumer that contains an “accidental overpayment” or other overage. The scammer asks the consumer to wire back the excess money. The check appears real and “clears,” so the consumer thinks it is okay to withdraw funds, but weeks later the bank discovers the check is phony. The consumer now owes the withdrawn funds to the bank.

4 HOME IMPROVEMENT

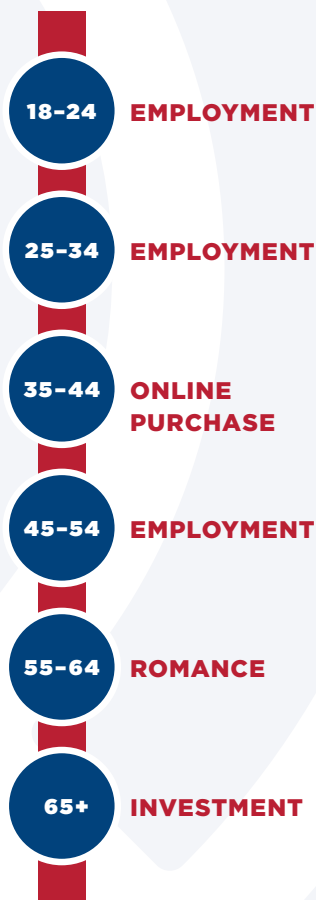
Door-to-door solicitors offer quick, low-cost repairs and then either take payments without returning, do shoddy work, or “find” issues that dramatically raise the price.

5 ADVANCE FEE LOAN

A loan is “guaranteed,” but comes with upfront charges, including taxes or “processing fees.” When the charges are paid, the loan never materializes and the applicant is left with larger debts.

50,559 Scams REPORTED IN 2018

RISKIEST SCAM BY AGE



RISKIEST SCAM BY GENDER



EMPLOYMENT

was the **RISKIEST SCAM** for both Military/Veterans and Students



ONLINE PURCHASES

was both the **MOST COMMON SCAM** (largest exposure) and **SCAM TYPE WITH THE MOST VICTIMS** (highest susceptibility)



PHONE

TOP MEANS OF CONTACT used to approach victims



CREDIT CARD

TOP MODE OF PAYMENT requested by scammers

TABLE 1

SNAPSHOT OF 2018 COMPARED WITH 2017/2016



PHONE remained the top means of contact from 2016 to 2018



CREDIT CARD remained the top method of payment from 2016 to 2018

* Note: In 2017, 10,670 “Can You Hear Me Now” scams were reported, significantly increasing reported scams from 2016 to 2017. Because none of those scams resulted in a monetary loss, we are not sure this was an actual scam. If we correct for that bump (removing the 10,670 reports from the 2017 total), we see that the increase in number of scams from 2017 to 2018 was about 36 percent (up from 37,157 scams in 2017).

BBB Risk Index

A Three-Dimensional Approach to Measuring Scam Risk

In the inaugural *2016 BBB Scam Tracker Risk Report*, we introduced the BBB Risk Index (Figure 2) 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 that simply being exposed to a scam is not the most significant aspect of scam risk. Whether the target falls for the scam (susceptibility) and how much money they lose are critical components of 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 all 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. The BBB Risk Index is calculated using data collected through BBB Scam Tracker, which is 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 underreporting of scams. Moreover, although local BBBs review reports to determine whether they describe what a reasonable person would believe to be a scam, these reviews do not validate consumer allegations. The Risk 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 BBB Risk Index.

The information provided by the BBB 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



The information provided by the BBB 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.

subgroups of the population, such as military families and students, and by age. To better understand the rationale for the BBB Risk 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 will succumb to the ploy. These scams reach a broad 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, and a scheme with relatively few victims may be of great concern if median losses are extremely high. The BBB Risk Index captures these real-world elements by representing the intersection of exposure, susceptibility, and monetary loss.

FIGURE 2

BBB RISK INDEX FORMULA

The formula for calculating the BBB Risk Index for a given scam type in a given population is **Exposure x Susceptibility x (Median Loss / Overall Median Loss) x 1,000**. The 2018 overall median loss was \$152. For purposes of calculating the BBB Risk Index, monetary loss is divided by the overall median dollar amount of losses reported to BBB Scam Tracker. This step controls for currency fluctuations to ensure that results can be compared over time and across currencies. As a final step, the result was multiplied by 1,000 to clear decimals and increase sensitivity.

Risk Index Elements Defined

EXPOSURE is a measure of the prevalence of a scam type,

BBB RISK INDEX



EXPOSURE

calculated as the percentage of all scams reported, represented by that scam type. This calculation includes scam reports made 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, whereas a relatively low exposure measure indicates that a scam type is less common.

SUSCEPTIBILITY is a measure of the likelihood of losing



SUSCEPTIBILITY

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, and 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.



MONETARY LOSS

10 Riskiest Scams

Table 2 lists the 10 riskiest scam types based on all reports submitted to BBB Scam Tracker in 2018. Most of the scam types named as the 10 riskiest remained the same as those in the top 10 in 2017, with the exception of romance scams moving up the list from the 11th spot to number 6 and family/friend emergency scams dropping off the top 10 list to number 13.

Employment scams took over the #1 spot this year as the riskiest scam in 2018, up from number 3 in 2017. Although susceptibility to employment scams remained about the same, the number of employment scams increased from 5.1 percent of scams reported in 2017 to 9.1 percent of reported scams in 2018; the median dollar loss jumped from \$800 in 2017 to \$1,204 in 2018.

TABLE 2
RISKEST SCAMS OF 2018

RANK		SCAM TYPE	BBB RISK INDEX	EXPOSURE		SUSCEPTIBILITY		MEDIAN \$ LOSS	
2018	2017			2018	2017	2018	2017	2018	2017
1 ↑	3	Employment	98.7	9.1% ↑	5.1%	13.7% ↓	13.8%	\$1,204 ↑	\$800
2 ↓	1	Online Purchase	76.6	20.6% ↑	9.7%	75.2% ↑	72.5%	\$75 ↓	\$100
3 ↑	5	Fake Check/ Money Order	58.0	4.0 ↑	2.3	14.6% ↑	14.2%	\$1,500 ↑	\$1,488
4 ↑	6	Home Improvement	57.6	1.0% ↑	0.8%	52.8% ↑	44.9%	\$1,745 ↑	\$1,225
5 ↓	4	Advance Fee Loan	57.6	3.0% ↑	2.2%	42.8% ↑	38.9%	\$675 ↑	\$600
6 ↑	11	Romance	54.7	0.8% ↓	0.3%	44.4% ↓	45.1%	\$2,500 ↑	\$1,500
7	7	Tech Support	44.2	5.3% ↑	4.8%	31.7% ↑	26.4%	\$403 ↑	\$300
8 ↓	2	Investment	42.7	0.5%	0.5%	62.4% ↑	50.8%	\$1,965 ↓	\$2,310
9 ↓	8	Travel/ Vacation	40.7	1.0% ↓	5.4%	32.7% ↑	3.7%	\$1,875 ↑	\$1,184
10	10	Government Grant	24.7	4.4% ↑	4.1%	14.3% ↑	10.3%	\$600 ↑	\$500

Employment Scams

Utilize “High-Touch” Approach

Employment scams are a good example of the “high-touch” approach, where scammers take the time to prepare elaborate setups. Scammers conduct in-depth interviews via Google Hangouts and other technologies, provide employment forms, and ask scam targets to perform job duties before the scam is discovered. These efforts appear to pay off, as evidenced by the higher median dollar loss. What makes these scams particularly risky is the fact that they made up 9.1 percent of all scams reported to BBB Scam Tracker in 2018. Employment scams target a large number of people and they tend to result in significant monetary loss.

The following excerpt is from a scam report submitted to BBB Scam Tracker in 2018:

“I was looking for work online and was contacted by this person telling me that they reviewed my resume and were interested in setting up an online interview with me for an administrative assistant position. The person stated that it would be a home-based position starting at \$20 an hour for two weeks of training, and after the training was done, they would pay \$30 an hour. This scammer told me that they [would] be sending me all the materials and their software so I [could] begin the training process. They sent a cashier’s check for \$3,911.35, which I needed to deposit and then wire transfer the funds to their vendor so they [could] send me the materials needed... The person told me that I had to buy 37 iTunes cards [worth] \$100 each with that money so they [could] upload the software to the cards and then I [could] download the software onto my computer... My bank ended up returning the check because it turned out to be fraudulent and my account was over-drafted by \$4,000 because of the overdraft fees.”

—Connecticut consumer, age 35–44

Although online purchase scams slipped to the number 2 riskiest spot, the number of online purchase scams submitted to BBB Scam Tracker in 2018 rose dramatically to 10,450 reports, up 124 percent from 4,655 in 2017. The only reason online purchase scams dropped to the number 2 spot on the list of 10 riskiest scams is because employment scam reports not only increased, but also

victims lost more money to those scams. The majority of online purchase scams occur when a payment is made online in exchange for goods or services, but nothing is delivered. The most common products promised but not delivered once payment is made include pets, automobile products, clothing, and cosmetics (Table 3).

TABLE 3

TOP PRODUCT CATEGORIES OF ONLINE PURCHASE SCAMS

RANK	PRODUCT	DETAILS	EXPOSURE	SUSCEPTIBILITY	MEDIAN \$ LOSS
1	Pets	Puppies, kittens, birds, exotic animals	26.2%	59.9%	\$600
2	Automobiles	Cars, car parts, motorcycles	14.9%	30.3%	\$272
3	Clothing	Clothing, jerseys, jewelry, shoes	26.4%	84.6%	\$51
4	Cosmetics	Skin creams, lotions, makeup, perfumes, soaps	10.0%	86.2%	\$110
5	Electronics	Cell phones, laptops, cases, headphones	9.4%	73.2%	\$83
6	Nutrition	Supplements/extracts for health, weight loss	3.4%	84.7%	\$150
7	Furniture	Lamps, rugs, clocks, blankets, candles	4.7%	88.1%	\$65
8	Tickets	Concert/event tickets	2.6%	88.8%	\$102
9	Hobby	Guns, bicycles, toys, collectibles	2.4%	71.5%	\$103



Pets Are #1 for Online Purchase Scams Again in 2018

The online sale of pets, including puppies, kittens, birds, and other animals, made up 26.2 percent of the products reported as online purchase scams to BBB Scam Tracker in 2018. Of those exposed to this scam, 59.9 percent lost money and the median dollar loss was \$600.

The following excerpt is from a scam report submitted to BBB Scam Tracker in 2018:

“I was looking to purchase a puppy. I [noticed] the price of the puppies [was] quite expensive, ranging from \$2,500–\$3,800. When I ran across this website, ‘Border Collie Paradise,’ the puppies were only \$600 with a transport fee of \$99. Of course, this was a very attractive offer. I contacted the seller through email. The seller wanted me to use Western Union to wire the money (that’s another warning sign). After sending them the money, the seller contacted me to tell me I needed to wire an additional \$1,250 for insurance to transport the dog. At that point, the warning signs were too glaring to ignore. I told them I wanted a refund...that was the last I ever heard from them... Please, do not ignore these warning signs. The puppies pictured on this website look as though they were cut out from a dog lovers’ calendar. It’s funny, I [went] back to the website several months later and the puppies are still 8 weeks old, and they still have the same puppies with the same names. Don’t ignore the warning signs of this pet scam!”

—California consumer, age 55–64

A large number of reports were again submitted in 2018 about so-called free trial offers. Consumers sign up for free trials of products such as cosmetics or weight-loss items, only to find they've agreed to a subscription if they don't return the product within a certain time period.

Are Free Trials Really Free?

Read Our Tips on How to Avoid a Subscription Trap

Online purchase scam reports include a large number of so-called free trial offers. Many free trial offers come with fine print buried on the order page or behind a link that gives consumers only a short period of time to receive, evaluate, and return the product to avoid being charged. In addition, the same hidden information may state that by accepting the free trial offer, the consumer is signing up for monthly shipments of the products and that fees will be charged to their credit card. Many people find it difficult to contact the seller to stop recurring charges, halt shipments, and get refunds.

When ordering online, don't click too fast. Review the order form. Look for pre-checked boxes. You may be giving permission to send more products that you'll have to pay for if you don't cancel, or you may be agreeing to a strict cancellation policy and not know it.

Be sure to research any company via [BBB.org](https://www.bbb.org) prior to placing an order. BBB issued a full report about free trial offers in 2018: *Subscription Traps and Deceptive Free Trials Scam Millions with Misleading Ads and Fake Celebrity Endorsements*, BBB International Investigations Initiative, 2018. us.bbb.org/freetrial

BBB suggests you ask the following questions:

Is the free trial offer related to a membership, subscription, or extended service contract?

Do I have to contact the company to avoid receiving more merchandise or services?

Who do I contact to cancel?

Will I receive other products with the free item? If so, will I have to pay for them or send them back if I do not want them? How long do I have to decide before incurring a charge?

Is there a membership fee? If so, is it refundable?

Will you automatically bill my credit card for anything?

Who is offering the trial—you or another company? What is the name and address of the company?

Fake check/money order scams increased from the number 5 riskiest scam in 2017 to number 3 in 2018. Although susceptibility stayed about the same, fake check/money order scams increased from 2.3 percent of all scams reported in 2017 to 4.0 percent in 2018. The median dollar loss for fake check/money order scams in 2018 remained high (\$1,500) relative to other scam types.

Fake Checks Are a Top Tactic for Employment, Investment, Sweepstakes, and Other Scams

Two Things to Remember Before You Cash a Check

Fake check/money order scams were the third riskiest scam in 2018. It is important to remember that fake checks are a common tactic scammers use in other types of scams.

“Buyers” send a check for more than the full price to sellers of cars or other items on Craigslist and other online classifieds sites. **“Employers”** send a check to “new hires” to buy supplies needed to do the job from home. **Sweepstakes or lottery “winners”** are given a check to pay taxes so the award can be delivered.

The check is almost always written for more than is required. The scam target is typically told they were overpaid and should send money from their bank account to another account or back to the scammer, or send prepaid cards to the scammer. By the time the target realizes the check they deposited is fake, they’ve already transferred money from their account.

Before you cash a check, remember two things:

1 Having the funds credited to a bank account does not mean the cashed check is valid.

Federal banking rules require that when someone deposits a check into an account, the bank must make the funds available right away—or within a day or two. But the bank also has the right to recover the money from the account holder if the check turns out to be counterfeit. Only when the check works its way back to the bank that supposedly issued it is it discovered to be counterfeit.

2 Cashier’s checks and postal money orders can be forged.

A cashier’s check is a check guaranteed by a bank, drawn on the bank’s own funds, and signed by a cashier. Cashier’s checks are treated as guaranteed funds because the bank itself, rather than the individual account holder, is responsible for paying the amount of the check. Cashier’s checks are commonly required for real estate and brokerage transactions. If a person deposits a cashier’s check, the person’s bank must credit the account by at least \$5,000 the next day. The same holds true for postal money orders. But both these types of supposedly guaranteed funds can be counterfeited.

If you do deposit a seemingly random check, one that is not from a friend or family member and has nothing to do with payroll, wait at least two weeks to be sure it cleared before spending any of it. This way, if it is fake and it bounces, at least you will not be out any of your money. If the person who sent you the check starts pressuring you to use the money right away, that is a warning sign that it may be a scam.

Demographics

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 helps us better understand how the nature of risk varies across different subgroups of the population. This information can be applied in targeting prevention efforts and informing outreach/educational strategies.

Age

The data show a significant difference between older adults and younger adults both in median dollars lost and susceptibility (Figure 3). An inverse relationship exists, where the median dollar loss increased with age (\$92 for ages 18-24 up to \$400 for ages 65+), and susceptibility decreased with age (42.4% for ages 18-24 down to 20.8% for ages 65+).

This may be a function of the types of scams different age groups are most susceptible to or are targeted by, or it may be related to differences in access to financial resources with increasing age. Table 4 highlights the three riskiest scams by age.

FIGURE 3

SUSCEPTIBILITY AND MEDIAN LOSS BY AGE

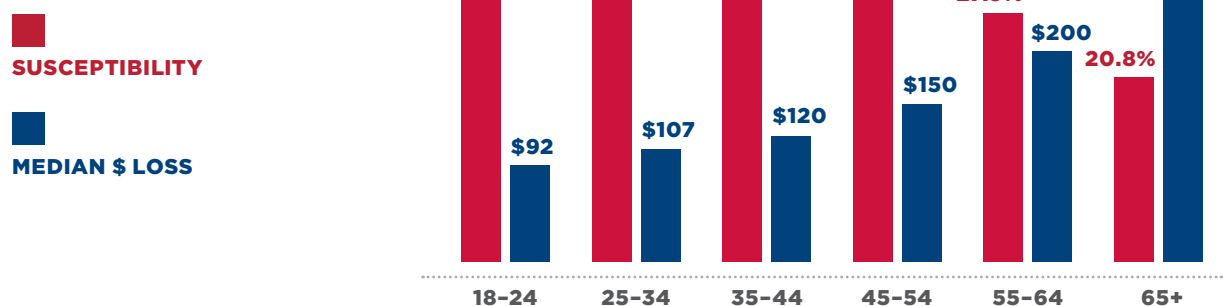
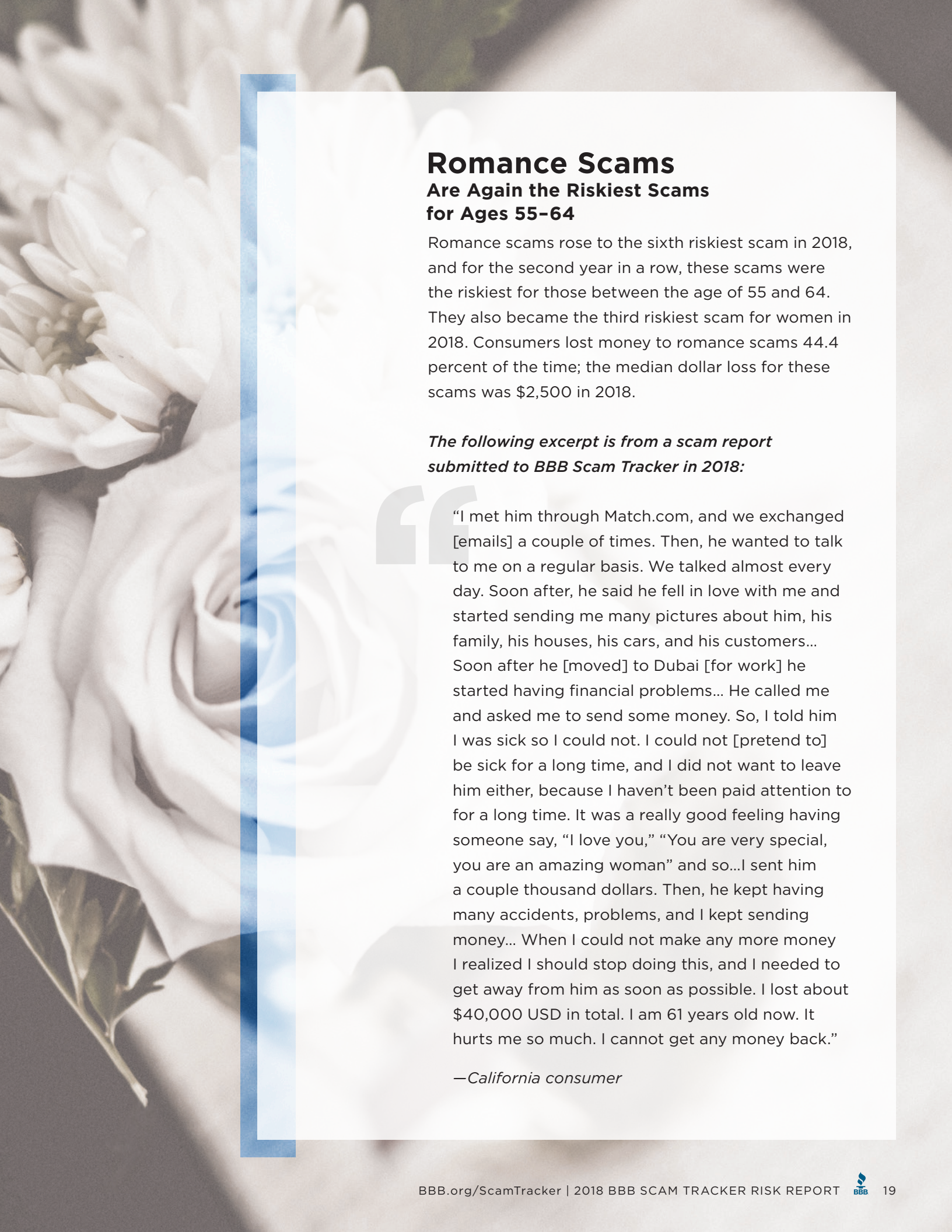


TABLE 4

3 RISKIEST SCAM TYPES BY AGE RANGE

	18-24	25-34	35-44	45-54	55-64	65+
1	Employment	Employment	Online Purchase	Employment	Romance	Investment
2	Fake Check/Money Order	Online Purchase	Home Improvement	Home Improvement	Investment	Travel/Vacation
3	Online Purchase	Fake Check/Money Order	Advance Fee Loan	Online Purchase	Employment	Tech Support



Romance Scams Are Again the Riskiest Scams for Ages 55–64

Romance scams rose to the sixth riskiest scam in 2018, and for the second year in a row, these scams were the riskiest for those between the age of 55 and 64. They also became the third riskiest scam for women in 2018. Consumers lost money to romance scams 44.4 percent of the time; the median dollar loss for these scams was \$2,500 in 2018.

The following excerpt is from a scam report submitted to BBB Scam Tracker in 2018:

“I met him through Match.com, and we exchanged [emails] a couple of times. Then, he wanted to talk to me on a regular basis. We talked almost every day. Soon after, he said he fell in love with me and started sending me many pictures about him, his family, his houses, his cars, and his customers... Soon after he [moved] to Dubai [for work] he started having financial problems... He called me and asked me to send some money. So, I told him I was sick so I could not. I could not [pretend to] be sick for a long time, and I did not want to leave him either, because I haven’t been paid attention to for a long time. It was a really good feeling having someone say, “I love you,” “You are very special, you are an amazing woman” and so...I sent him a couple thousand dollars. Then, he kept having many accidents, problems, and I kept sending money... When I could not make any more money I realized I should stop doing this, and I needed to get away from him as soon as possible. I lost about \$40,000 USD in total. I am 61 years old now. It hurts me so much. I cannot get any money back.”

—California consumer

Gender

In 2018, women were more likely to report a scam to BBB Scam Tracker than men, similar to findings reported in the *2017 BBB Scam Tracker Risk Report*. Overall, susceptibility to losing money when exposed to a scam was similar for both men and women at 29.1 and 30.5 percent respectively. However, median dollar loss for women remained substantially lower than for men (Figure 4). 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 three riskiest scams for men and women are listed in Table 5.

FIGURE 4

SUSCEPTIBILITY AND MEDIAN LOSS BY GENDER

Median \$ Loss



VS

% Susceptibility

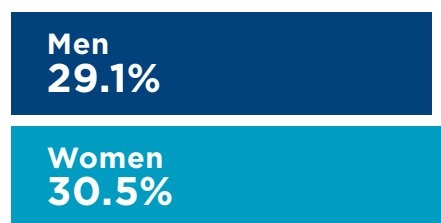


TABLE 5

3 RISKIEST SCAM TYPES BY GENDER

Men

Employment
Travel/Vacation
Home Improvement

..... **1**

..... **2**

..... **3**

Women

Employment
Online Purchase
Romance

Travel/Vacation Scams

Are Number 2 Riskiest Scam for Men

Travel/vacation scams rose to the number 2 riskiest scam for men in 2018. These scams make up only 1.0 percent of the total reported to BBB Scam Tracker in 2018, but when exposed to travel/vacation scams, consumers at large lost money 32.7 percent of the time, and the median dollar loss was \$1,875.

For men, the impact was much greater, as they reported a loss in 37.4% of reports and the median dollars lost was \$3,950—more than three times the median dollars lost for women (\$1,200).

The following excerpt is from a scam report submitted to BBB Scam Tracker in 2018:

“This company called me with a great offer to buy my timeshare in Mexico... Unfortunately, I signed a contract and that’s when the trouble began. They first asked for \$5,000 to get registered in Mexico, so I wired the money to an account in Mexico... Next, they said that there was state tax that I had to pay and it was \$23,000, so I stupidly sent that to Mexico as well... I got a copy of a letter stating that I had to pay another \$5,000 for some Mexico government regulations. I did this [and then received] another letter supposedly from the Mexico customs department saying that I had to pay another \$45,000 for a customs clearance, of which the buyer agreed to reimburse me 72 percent. Finally, I had enough. I checked with a timeshare lawyer in New Orleans who told me it was definitely a scam... Then, I called the resort to see what they knew and before I told them anything, they described the exact scenario to me as what had taken place. They said it was definitely a scam... Right now, I am out \$33,000, which I will never see again.”

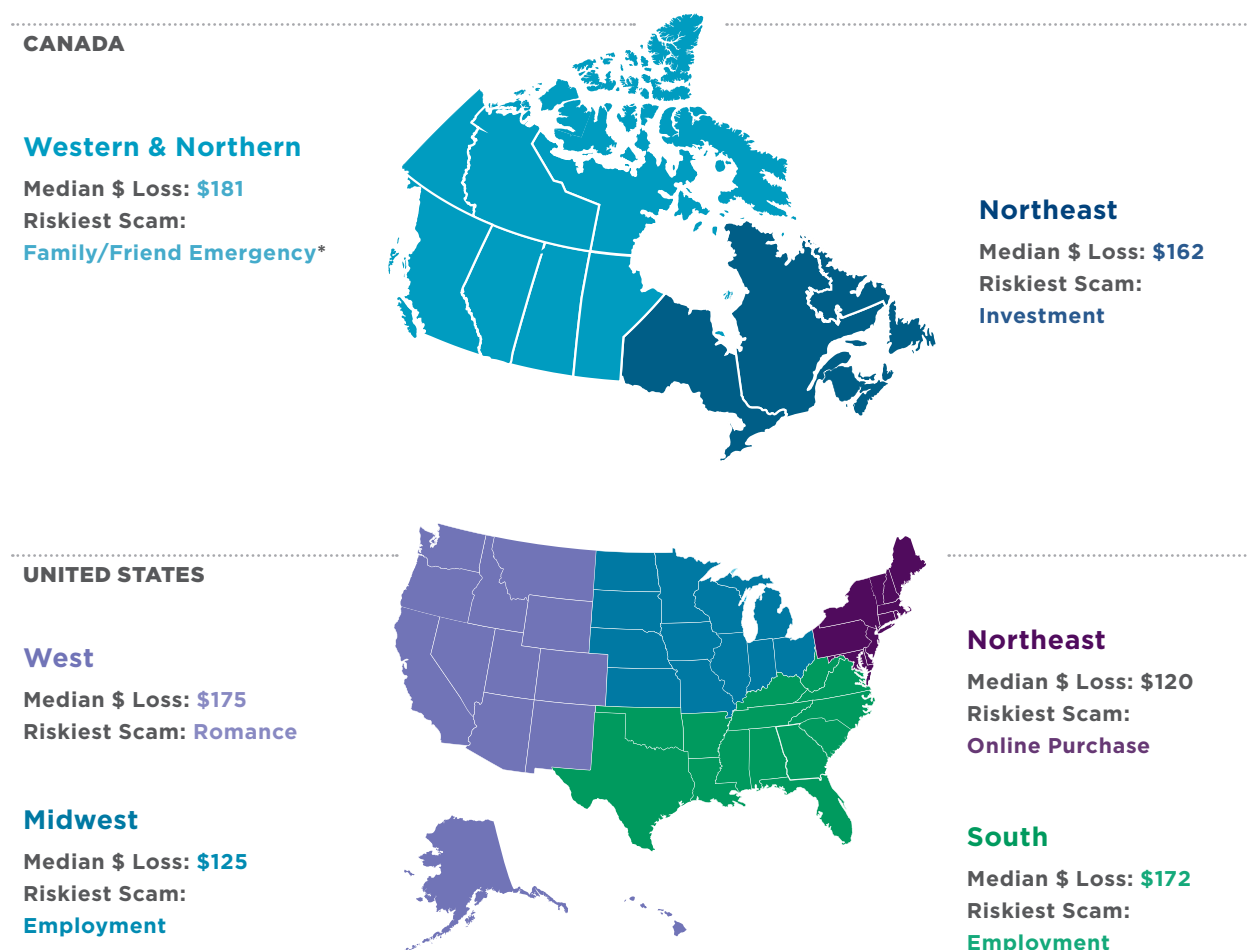
—Colorado consumer, age 65+

Geographic Area

As broken out below, scams show some variability by region (Figure 5). This may be an indication that scammers are more active in certain areas and may also reflect demographic and socioeconomic differences by regions that in turn correlate with different types of scams and differing levels of susceptibility and loss. Please note that these data points refer to the location of the person reporting the scam, not the location of the perpetrator of the scam. Although location information about perpetrators is provided in some cases, the accuracy of this information varies because most victims and targets are uncertain of the location of the perpetrator and are often given false information with respect to the scammer's location.

FIGURE 5

RISKIEST SCAM TYPES BY GEOGRAPHIC AREA



* Note: There were only two reports in this category that resulted in a loss; the second riskiest scam type for Canada's Western & Northern region was investment scams.

Scam Delivery and Payment Methods

Website Overtakes Phone as Top Means of Contact with Monetary Loss *Online Exposure Appears to Increase Likelihood of Losing Money*

Scammers continue to exploit the full range of communications to connect with their targets and readily adapt the latest technologies to perpetrate scams.

Figure 6 provides a comparison of all scam delivery methods with a monetary loss reported to BBB Scam Tracker in 2018. In 2018, for the first time, website (25 percent) eclipsed phone (17 percent) as the top means of contact for scams with a monetary loss. In 2017, phone and website were equal; in 2016, phone eclipsed website. Also notable this year, social media increased to 20 percent, up from 13 percent in 2017 and 11 percent in 2016.

Credit cards remained the top payment method requested by scammers in

2018 (Figure 7). Bank account debit, wire transfers, and prepaid cards were also key methods used by scammers. Criminals continue to utilize these methods because they are more difficult to trace. For this

reason, payment methods such as wire transfers and prepaid cards should be considered a red flag for fraud. Online payment systems rose from 8 percent in

2017 to 13 percent in 2018. This shift is not surprising, considering the continued increase in online transactions. This year, BBB Scam Tracker added a new payment method category for cryptocurrency, which currently makes up 1 percent of the total payment methods reported.

One notable finding in 2018 (Figure 8) is that when initial means of contact with no monetary loss is compared with initial means of contact with a monetary loss, consumers who

are approached online (email, website, social media, internet messaging, and online classifieds) are more likely to lose money. If approached by phone, they appear to be less likely to lose money.



Criminals continue to utilize these methods because they are more difficult to trace. For this reason, payment methods such as wire transfers and prepaid cards should be considered a red flag for fraud.

FIGURE 6

MEANS OF CONTACT WITH \$ LOSS (% TOTAL)

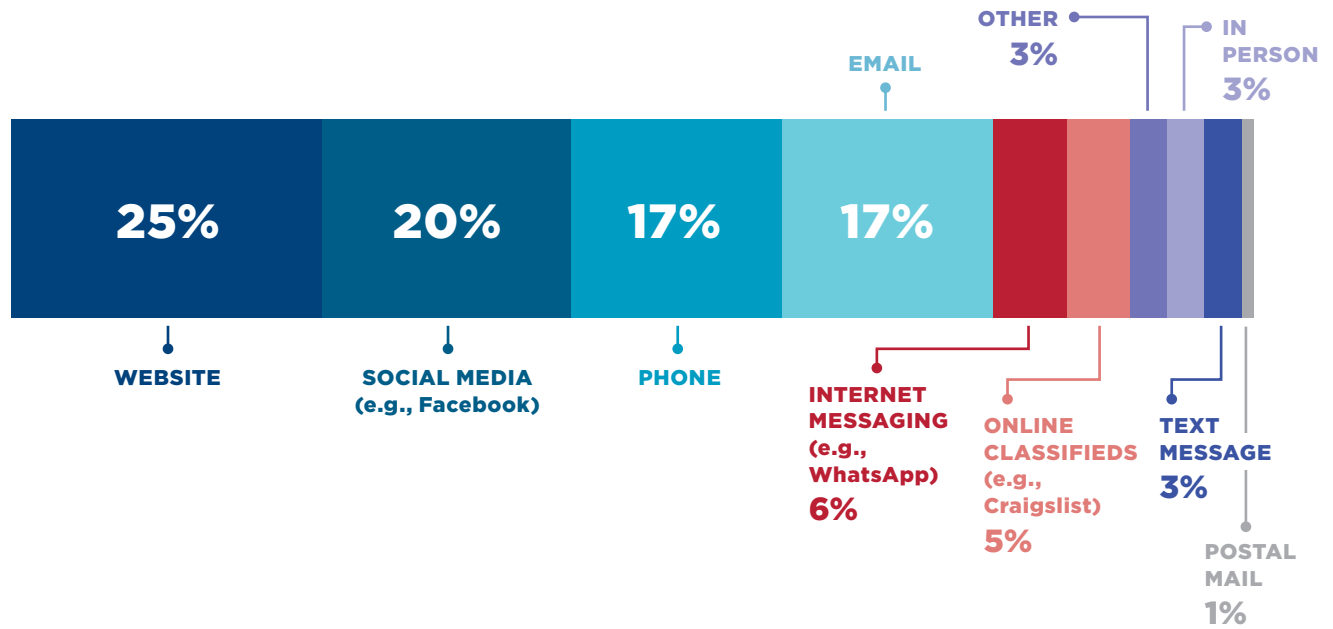


FIGURE 7

PAYMENT METHOD USED BY VICTIMS (% TOTAL)

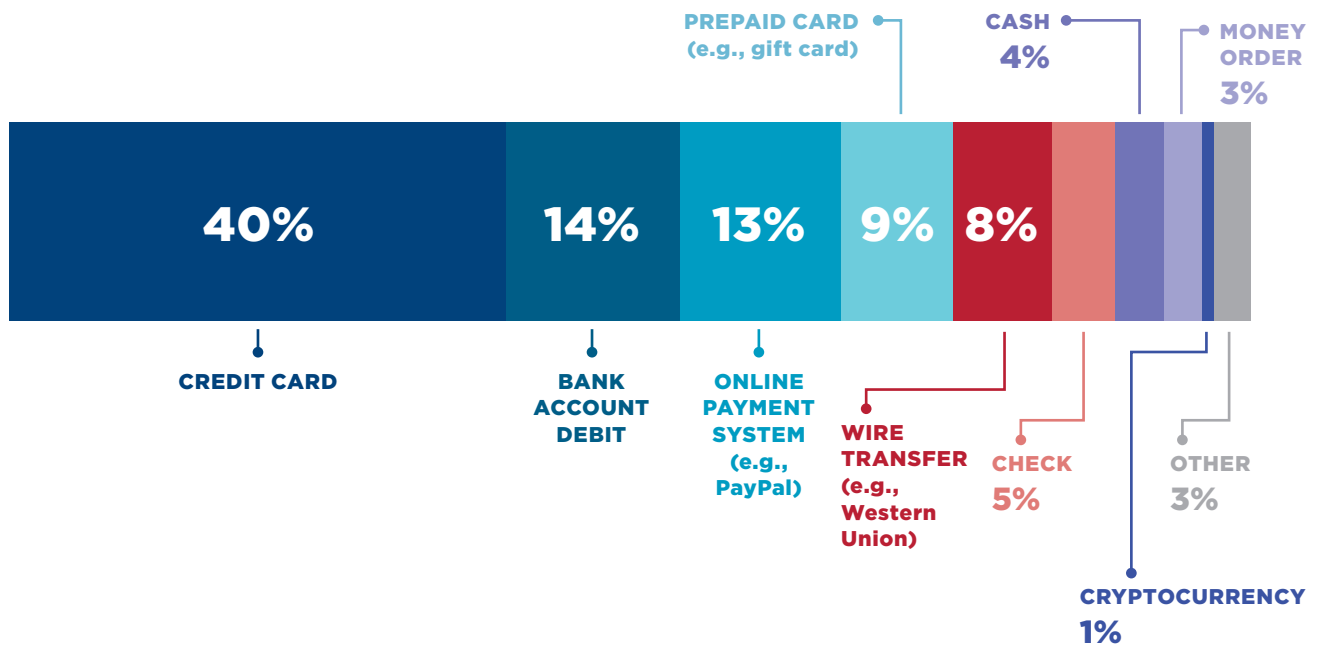
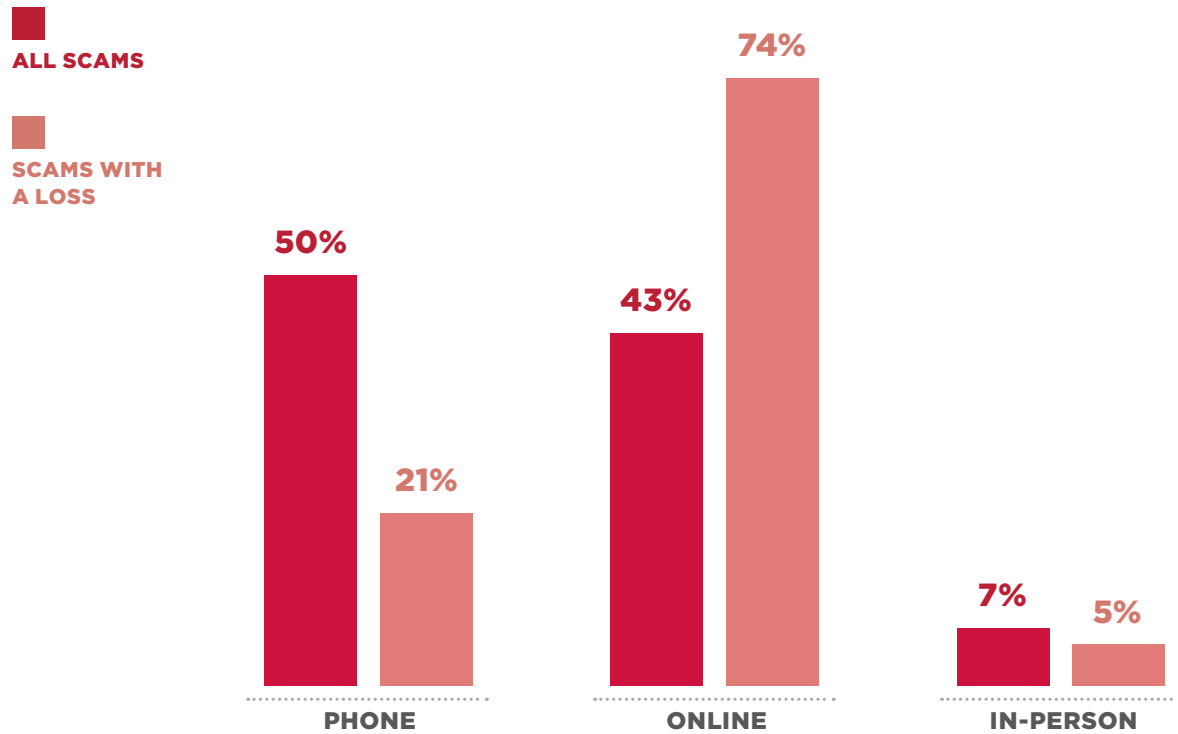


FIGURE 8

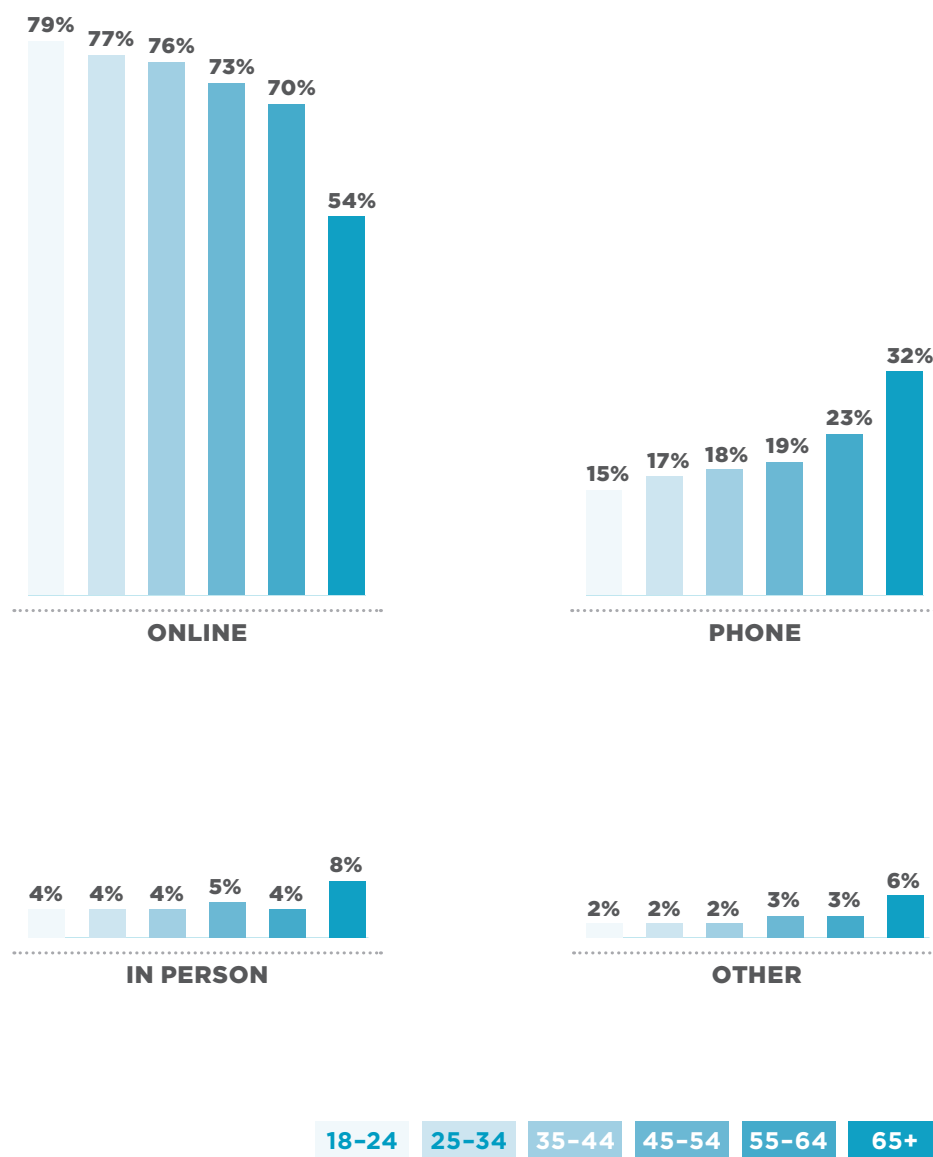
**ALL SCAMS COMPARED WITH SCAMS WITH A LOSS (% TOTAL)
BY MEANS OF CONTACT**



* Note: Categories include Phone (phone + text messaging), Online (email + website + social media + internet messaging + online classifieds), and In Person (in person + postal mail + fax).

All ages were more likely to lose money when approached online. However, younger adults were more likely to fall for scams that used online means of contact (website, email, internet messaging, online classifieds, social media) than were older adults, whereas those age 65+ were more likely to fall for scams that used phone or in-person contact methods than younger adults (Figure 9).

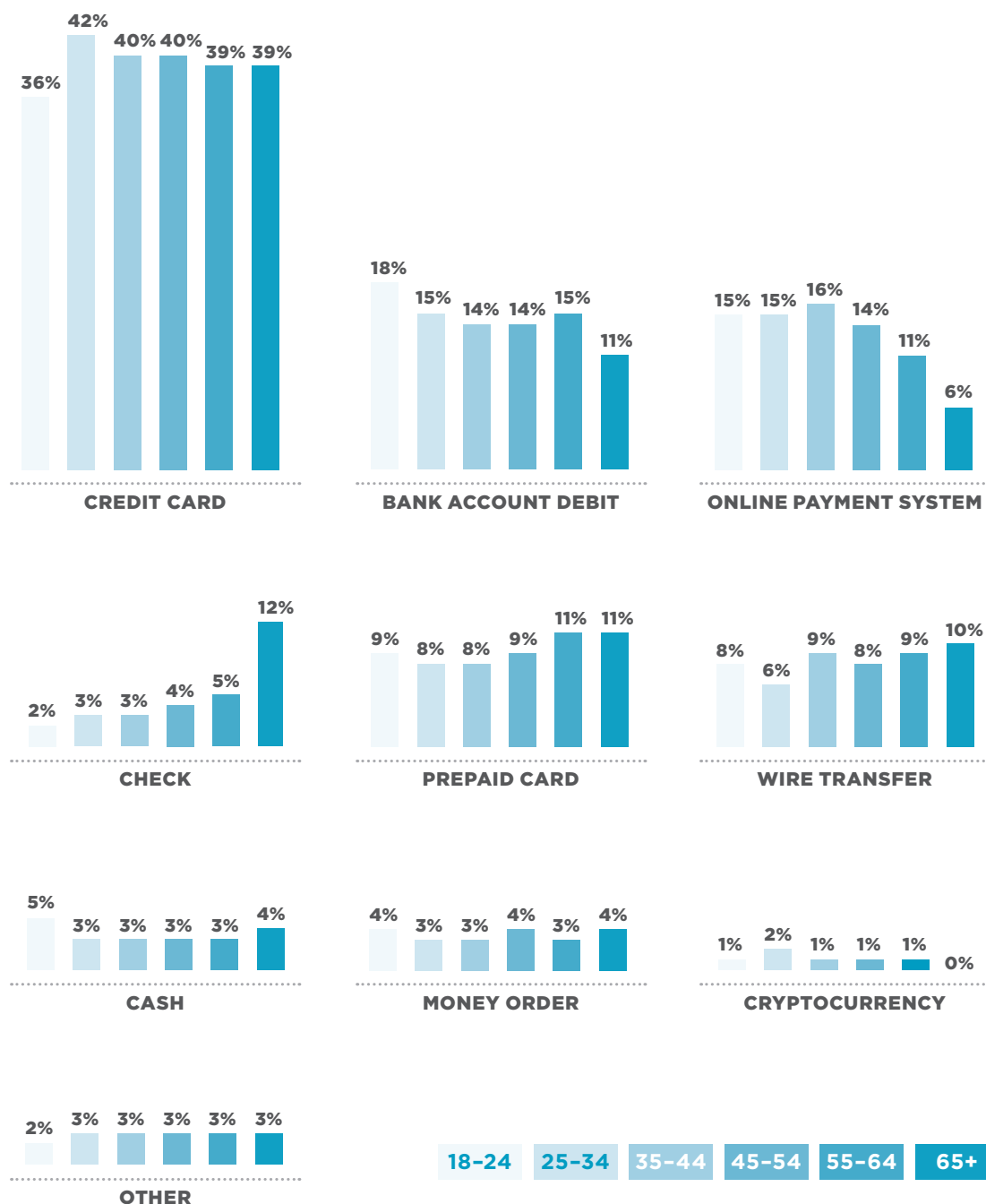
FIGURE 9
MEANS OF CONTACT WITH \$ LOSS BY AGE (% TOTAL)



The most common payment method remained credit card consistently across all age ranges. While most payment methods were similar for all age segments, younger adults were slightly more likely to pay via bank account debit and online payment system than were older adults, and older adults were slightly more likely to pay via check or prepaid card (Figure 10).

FIGURE 10

PAYMENT METHODS BY AGE (% TOTAL)



Spotlight on Military Families and Veterans

It has long been recognized that military families and veterans are at increased risk of being targeted by scammers. Active-duty military personnel are targeted for their youth and steady paychecks, and military families are often required to put faith in others while juggling deployment and frequent moves, which leaves them particularly vulnerable. Individuals who self-identified as being active-duty military personnel, spouses, or veterans represent 9.4 percent of reports submitted to BBB Scam Tracker in 2018. Although the susceptibility of the military community was similar to the susceptibility of non-military, active military, veterans, and military spouses had a median loss of \$200 when falling victim to a scam, which is 33.3 percent higher than non-military consumers (Figure 11). The BBB Risk Index has been applied to identify the three riskiest scams for military families and veterans (Table 6).

FIGURE 11

MEDIAN \$ LOSS AND SUSCEPTIBILITY OF MILITARY FAMILIES AND VETERANS VERSUS NON-MILITARY

Median \$ Loss



VS

% Susceptibility

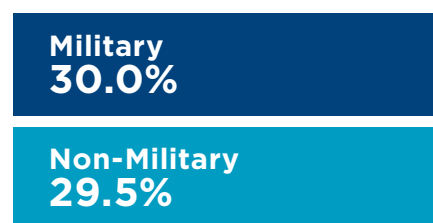


TABLE 6

3 RISKIEST SCAMS: MILITARY FAMILIES AND VETERANS VERSUS NON-MILITARY

Military/Veterans

Employment
Home Improvement
Online Purchase

..... **1**

..... **2**

..... **3**

Non-Military

Employment
Online Purchase
Fake Check/Money Order

Home Improvement Scams Remain Second Riskiest Scam for Military Families and Veterans

Home improvement scams were the number 2 riskiest scam for military families and veterans, behind employment scams, in 2018. Overall, home improvement scams were the number 4 riskiest scam in 2018, up from number 6 in 2017. For this scam, military consumers are more likely both to lose money (59.7 percent susceptibility vs. 52.8 percent overall) and to lose higher dollar amounts (\$2,000 vs. \$1,745 overall median dollars lost). It's possible, given the fact that military families move more often than do average consumers, they are more susceptible to these types of scams.*

The following excerpt is from a scam report submitted to BBB Scam Tracker in 2018:

“The company knocked on my door wanting to look on my roof for hail damage. When they came down, I was advised that they thought there was a claim. They said if I signed a contract, they would pursue the insurance company to get a claim. To my surprise, they did obtain a claim... Since then, they do not answer phones and have since FORGED my signature, my wife's signature, and the mortgage company's signature. The amount of the check was for \$9,400. Absolutely no work was done on my roof.”

—Military consumer in Illinois, age 55–64

* *The Demographics of Military Children and Families*, Molly Clever and David R. Segal, 2013.
<https://pdfs.semanticscholar.org/c567/b17bc58e83e93e68e28f1cfe270473593a48.pdf>

Spotlight on Students

Students Tend to Be More Susceptible to Scams Than Non-Students, but Lose Less Money

Individuals who self-identified as students represented 9.4 percent of reports submitted to BBB Scam Tracker in 2018. These individuals continue to be more vulnerable when exposed to a scam: 41.6 percent of students reported a loss when exposed to a scam as compared to 28.3 percent of non-students (Figure 12). However, the median dollar loss of \$102 for students is significantly lower than the median dollar loss for non-students of \$161 (Figure 12). This trend reflects the insights we highlighted in 2017. Once again, these findings may reflect differences in the scam types to which students are most vulnerable 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 overall 18-24 age category into which most students fall. Table 7 includes the riskiest scams for students.

FIGURE 12

MEDIAN \$ LOSS AND SUSCEPTIBILITY OF STUDENTS VERSUS NON-STUDENTS

Median \$ Loss



VS

% Susceptibility

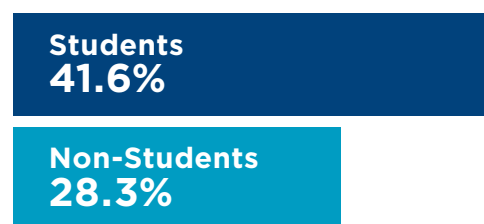


TABLE 7

3 RISKIEST SCAMS: STUDENTS VERSUS NON-STUDENTS

Students

Employment
Fake Check/Money Order
Online Purchase

..... **1**

..... **2**

..... **3**

Non-Students

Employment
Online Purchase
Home Improvement

Employment/Fake Check Scams Continue to Be Riskiest Scams for Students

In 2018, employment and fake check/money order scams were again the number 1 and number 2 riskiest scams for students; these scams were also the riskiest scams for consumers in the 18-24 age category. Considering this age group is more likely seeking both part-time and full-time employment, they are perhaps more vulnerable to these types of scams. Another factor that may play into the vulnerability of younger adults to these scams is the fact that the use of checks is in rapid decline, disrupted by digital payments, the internet, and technology in general.* For this reason, younger people with less check experience may not fully understand how checks work. See page 17 for tips on fake checks.

The following excerpt is from a scam report submitted to BBB Scam Tracker in 2018:

“Was emailed to my school email, the email stated he was a professor at my university and was looking to employ some students over the summer so he would pay about \$620 for about three or four days of work and then he would also pay us for the things he made us buy. His instructions were to complete little tasks to help him while he was away. So he told me he needed to buy iTunes cards to use with the students he was helping and told me to buy him 15 cards each worth \$100 so he sent me a check to cover that and to deposit into my bank and so I did, however, about a week later the checks bounced and I figured out I had been scammed.”

—California student, age 18-24

* The 2013 Federal Reserve Payments Study: Recent and Long-Term Trends in the United States: 2000-2012, Detailed Report and Updated Data Release, Federal reserve System, July 2014.
<https://frbervices.org/assets/news/research/2013-fed-res-paymt-study-detailed-rpt.pdf>.

Spotlight on Impersonated Organizations

Scammers Continue to Co-opt Household Brand Names to Perpetrate Scams

One of the most common methods a scammer uses is “impersonation.” By pretending to be legitimate businesses, agencies, and organizations that are well known and trusted by the consumer, scammers are able to better manipulate their targets (Table 8).



IRS Scams

The scammer pretends to be the Internal Revenue Service or Canada Revenue Agency.



Government Grant Scams

The scammer pretends to be a government agency.



Tech Support Scams

The scammer pretends to be a well-known technology company such as Microsoft or Apple.



Sweepstakes, Lottery, Prize Scams

The scammer pretends to be a well-known company that distributes sweepstakes or lottery winnings, such as Publishers Clearing House.



Travel/Vacation Scams

The scammer pretends to be a well-known travel brand.



Credit Card Scams

The scammer pretends to be a well-known bank or credit card company.

TABLE 8

TOP 15 LEGITIMATE ORGANIZATIONS/BRANDS USED FOR IMPERSONATION

- 1 **U.S. Internal Revenue Service**
.....
- 2 **U.S. Government / All Other Agencies**
(Treasury, Reserve, Medicare, Social Security, Grants)
.....
- 3 **Publishers Clearing House**
.....
- 4 **Microsoft**
.....
- 5 **Apple**
.....
- 6 **Amazon**
.....
- 7 **Cash Advance/Advance America**
.....
- 8 **Canada Revenue Agency**
.....
- 9 **Facebook**
.....
- 10 **Ray Ban**
.....
- 11 **Better Business Bureau**
.....
- 12 **PayPal**
.....
- 13 **Bank of America**
.....
- 14 **Secret Shopper**
.....
- 15 **Yellow Pages**
.....

* Note: Other legitimate organizations included on the full list are TripAdvisor, DirectTV, AT&T, Google, the FBI, Mega Millions, Internet Domain Name Service (IDNS), Marriott, and the IMF.

IRS Again Most Impersonated Entity in 2018

Followed by Other Government Agencies

Almost 2,300 IRS impersonation scams were reported to BBB Scam Tracker in 2018, making up the bulk of the 3,626 tax collection scams. More than 1,300 scams reported to BBB Scam Tracker mentioned impersonations of other government agencies. Government grant scams remained on the list of 10 riskiest scams for the second year in a row; these scams are perpetrated when scammers pretend to represent government agencies to offer free, guaranteed government grants.

The following excerpt is from a scam report submitted to BBB Scam Tracker in 2018:

“Days after receiving a letter from the IRS in the mail (which looked 100 percent legitimate), three days later I was called by the ‘IRS’ on the phone and told I was being sued for tax fraud and evasion, and that in the next 15 minutes my entire life would be taken away and I would be going to jail. Over the next 22 hours, I was held hostage electronically and emotionally [on the phone]... I am a smart and accomplished woman. These people are scary and totally believable. They have it down to a science.... Even hanging up the phone was scary.”

—New York consumer, age 45-54

KNOW Scams

Though scams and scammers continue to plague the marketplace, consumers can learn some key strategies that

will enable them to avoid falling prey to scams. In fact, over 70 percent of reports to BBB Scam Tracker in 2018 were from non-victims. Thanks to the thousands of citizen heroes who reported scams, we can glean helpful information that will assist consumers in avoiding fraudsters.



Thanks to the thousands of citizen heroes who reported scams, we can glean helpful information that will assist consumers in avoiding fraudsters.

10 TIPS for Avoiding a Scam

If you can remember the following tips, 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 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. Even then, the site could be shady. Check out the company first at [BBB.org](https://www.bbb.org).
- 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 transactions when making payments for goods, services, taxes, and debts.
- 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](https://www.bbb.org/AvoidScams).



Conclusion

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 also may 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 *2018 BBB Scam Tracker Risk Report* is a critical part of our ongoing work to contribute new, useful data and analysis to further the efforts of all who are engaged in combatting marketplace scams. We will continue our work to reduce the impact of scams to help consumers and legitimate businesses prosper in a trustworthy marketplace.

About BBB Institute

The *2018 BBB Scam Tracker Risk Report* is published each year by the BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the Better Business Bureau. BBB Institute works with local, independent BBBs across North America to deliver educational programs that foster a trusted marketplace by:

- Empowering consumers to take control of their purchasing decisions and avoid scams.
- Helping businesses deliver excellent service with integrity and become integral stakeholders in their communities.
- Publishing research that provides critical insights for the average consumer and informs how we develop and deliver our programs.

You can find more information about BBB Institute and its programs at

BBBMarketplaceTrust.org.

BBB Research

Timely Data Informs Consumer Education Efforts

Tech-Savvy Scammers Work to Con More Victims: 2018 BBB Scam Tracker Risk Report is the third annual report published by BBB Institute that highlights the year's riskiest scams. We are committed to delivering new and timely research that enables us to continue creating and delivering programs that empower both consumers and businesses to avoid falling prey to scams.⁴

Our first research report, *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*,⁵ surveyed consumers in the United States and Canada to identify the stereotypes and misperceptions around scam victimization that are barriers to effective outreach to at-risk populations.

In early 2018, BBB Institute partnered with the Council of Better Business Bureaus, Inc., to publish *Scams and Your Small Business*.⁶ The report used both BBB Scam Tracker data and an outside panel to provide insights on scams targeting small businesses.

In 2019, BBB Institute will partner with FINRA Foundation and the Stanford Center on Longevity to release new research that more closely examines the factors that contribute to individuals becoming victims of fraud. The goal of the study is to determine effective educational outreach that can help individuals avoid being defrauded by scams.

BBB Institute continues to explore new research that provides fresh and important insights regarding the scam landscape and use that information to work with our partners in business, law enforcement, government, and the not-for-profit sector to enhance our scam prevention efforts and spread awareness to consumers and businesses.

Special Thanks

The BBB Scam Tracker program is made possible thanks to the tireless and excellent work of BBBs across North America. The initial concept of BBB Scam Tracker came from a local BBB. The program exemplifies BBB Institute's work as a catalyst and spur for BBB innovation at the local and national levels. Dedicated staff working for local BBBs review and compile the consumer

⁴ BBB Institute's data and research can be found at www.bbbmarketplacetrust.org/resources#research.

⁵ *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*, Emma Fletcher and Rubens Pessanha, 2013. BBB.org/TruthAboutScams.

⁶ Find this report at BBB.org/SmallBizScams.

reports that fuel the BBB Scam Tracker tool. Without their vision and dedication, there would be no BBB Scam Tracker.

We'd also like to thank Warren King, president and CEO of the Better Business Bureau Serving Western Pennsylvania, who leads the BBB Scam Tracker Task Force, and its members, Jane Driggs, president and CEO of the Better Business Bureau Serving Northern Nevada and Utah, and Craig Turner, director of information systems of the Better Business Bureau Serving Eastern and Southwest Missouri and Southern Illinois. The work of the task force, with

support from BBB Institute's Melissa "Mel" Trumpower and Ayaz Minhas, is integral to the success of this program and the expansion of our research efforts.

We would also like to thank Matt Scandale, senior data analyst for the Council of Better Business Bureaus, for his exceptional talent in pulling the data from BBB Scam Tracker; and Katherine Hutt, director of communications for the Council of Better Business Bureaus, and Amy Gwiazdowski, director of internal strategic communications, for their support in getting the word out about our most recent findings.

APPENDIX A: Glossary of Scam Type Definitions

ADVANCE FEE LOAN	In this scam, a loan is guaranteed, but once the victim pays up-front charges such as taxes or a “processing fee,” the loan never materializes.
BUSINESS EMAIL COMPROMISE	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.
CHARITY	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 PRODUCT	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.
CREDIT CARD	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	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.
CRYPTOCURRENCY	These scams involve the purchase, trade, or storage of digital assets known as cryptocurrencies. Often these scams involve fraudulent Initial Coin Offerings (ICOs), a type of fundraising mechanism in which a company issues its own cryptocurrency to raise capital. Investors are scammed into paying money or trading their own digital assets when the scammer has no intention of building a company. Cryptocurrency scams also involve scenarios in which investors store their cryptocurrencies with fraudulent exchanges.
DEBT COLLECTION	In this con, phony debt collectors harass their targets, trying to get them to pay debts they don’t owe.
EMPLOYMENT	Victims of employment scams are led to believe they are applying or have just been hired for a promising new career when instead 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 CHECK/ MONEY ORDER	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	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	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.
FOREIGN MONEY EXCHANGE	In this scam, the target receives an email from a foreign government official, member of royalty, or a business owner offering a huge sum for help getting money out of the scammer’s country. The victim fronts costs for the transfer, believing that they will be repaid.
GOVERNMENT GRANT	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	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.

APPENDIX A: Glossary of Scam Type Definitions

HOME IMPROVEMENT	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 a victim’s personal information (e.g., Social Security number, bank account information, and credit card numbers) to pose as that individual for their own gain. Using the target’s identity, the thief may open a credit account, drain an existing account, file tax returns, or obtain medical coverage.
INVESTMENT	These scams take many forms, but all prey on the desire to make money without much risk or initial funding. “Investors” are lured with false information and promises of large returns with little or no risk.
MOVING	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.
ONLINE PURCHASE	These cons often involve purchases and sales, often on eBay, Craigslist, 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, if the scammer is the seller, they never deliver the goods.
PHISHING	These schemes employ communications impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information with which the scammer can gain access to bank accounts or can steal the recipient’s identity.
RENTAL	Phony ads are placed for rental properties that ask for up-front payments. Victims later discover the property doesn’t exist or is owned by someone else.
ROMANCE	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.
SCHOLARSHIP	This con hooks victims, often students struggling with tuition costs, with the promise of government scholarship money, but the up-front “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.
SWEEPSTAKES, LOTTERY, AND PRIZE	This con fools victims into thinking they have won a prize or lottery jackpot but must pay up-front fees to receive the winnings, which never materialize. Sometimes this con involves a fake check and a request to return a portion of the funds to cover fees.
TAX COLLECTION	In this 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.
TECH SUPPORT	Tech support scams start with a call or pop-up warning that alerts the target to a computer bug or other problem. Scammers posing as tech support employees of well-known tech companies hassle victims into paying for “support.” If the victim allows remote access, malware may be installed.
TRAVEL AND VACATION	Con artists post listings for properties that are not for rent, do not exist, or are significantly different from what’s pictured. In another variation, scammers claim to specialize in timeshare resales and promise they have buyers ready to purchase.
UTILITY	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	This con targets businesses, attempting to fool them into paying for a listing or ad space in a nonexistent directory or “Yellow Pages.” In some cases, the directory technically exists, but is not widely distributed and a listing is of little or no value—these directories are essentially props in the scammer’s ploy.

APPENDIX B: Scam Data Table

SCAM TYPE	# OF REPORTS	% EXPOSURE	% SUSCEPTIBILITY	MEDIAN \$ LOSS	RISK INDEX	TOP MEANS OF CONTACT WITH \$ LOSS	TOP PAYMENT METHOD
Advance Fee Loan	1,537	3.0%	42.8%	\$675	57.6	Phone	Prepaid Card
Business Email Compromise	267	0.5%	24.3%	\$560	4.8	Email	Credit Card
Charity	325	0.6%	15.1%	\$97	0.6	In Person	Check
Counterfeit Product	1,308	2.6%	56.0%	\$92	8.8	Website	Credit Card
Credit Card	1,393	2.8%	24.9%	\$100	4.5	Website	Credit Card
Credit Repair/Debt Relief	743	1.5%	26.2%	\$772	19.6	Phone	Bank Account Debit
Cryptocurrency	140	0.3%	63.6%	\$900	10.5	Website	Cryptocurrency
Debt Collection	2,896	5.7%	7.3%	\$400	11.0	Phone	Credit Card
Employment	4,605	9.1%	13.7%	\$1,204	98.7	Email	Credit Card
Fake Check/Money Order	2,037	4.0%	14.6%	\$1,500	58.0	Email	Check
Fake Invoice	1,143	2.3%	18.4%	\$250	6.8	Postal Mail	Check
Family/Friend Emergency	306	0.6%	16.3%	\$3,000	19.4	Phone	Prepaid Card
Foreign Money Exchange	163	0.3%	21.5%	\$962	4.3	Email	Wire Transfer
Government Grant	2,211	4.4%	14.3%	\$600	24.7	Phone	Prepaid Card
Health Care, Medicaid, Medicare	1,045	2.1%	5.9%	\$300	2.4	Phone	Credit Card
Home Improvement	479	1.0%	52.8%	\$1,745	57.6	In Person	Check
Identity Theft	791	1.6%	14.2%	\$300	4.4	Phone	Credit Card
Investment	271	0.5%	62.4%	\$1,965	42.7	Phone	Wire Transfer
Moving	118	0.2%	68.6%	\$800	8.3	Phone	Credit Card
Online Purchase	10,450	20.6%	75.2%	\$75	76.6	Website	Credit Card
Phishing	5,567	11.0%	4.8%	\$250	8.7	Phone	Credit Card
Rental	444	0.9%	34.2%	\$996	19.7	Online Classifieds	Wire Transfer
Romance	381	0.8%	44.4%	\$2,500	54.7	Social Media	Wire Transfer
Scholarship	21	0.0%	19.1%	\$100	0.1	Internet Messaging	Bank Account Debit
Sweepstakes, Lottery, Prize	2,062	4.1%	10.4%	\$500	13.9	Phone	Wire Transfer
Tax Collection	3,626	7.2%	1.6%	\$1,000	7.4	Phone	Prepaid Card
Tech Support	2,666	5.3%	31.7%	\$403	44.2	Phone	Credit Card
Travel and Vacation	514	1.0%	32.7%	\$1,875	40.7	Phone	Credit Card
Utility	554	1.1%	8.5%	\$500	3.0	Phone	Prepaid Card
Yellow Pages/Directories	128	0.2%	15.6%	\$430	1.1	Phone	Credit Card
Other	2,368	4.7%	23.8%	\$400	29.3	Phone	Credit Card
TOTAL REPORTS	50,559						

APPENDIX C: Top 10 Scam Types by Overall Risk, Exposure, Susceptibility, and Monetary Loss

	RISK	EXPOSURE	SUSCEPTIBILITY	MEDIAN \$ LOSS
1	Employment	Online Purchase	Online Purchase	Family/Friend Emergency
2	Online Purchase	Phishing	Moving	Romance
3	Fake Check/ Money Order	Employment	Cryptocurrency	Investment
4	Home Improvement	Tax Collection	Investment	Travel/ Vacation
5	Advance Fee Loan	Debt Collection	Counterfeit Product	Home Improvement
6	Romance	Tech Support	Home Improvement	Fake Check/ Money Order
7	Tech Support	Government Grant	Romance	Employment
8	Investment	Sweepstakes/ Lottery/Prize	Advance Fee Loan	Tax Collection
9	Travel/ Vacation	Fake Check/ Money Order	Rental	Rental
10	Government Grant	Advance Fee Loan	Travel/ Vacation	Foreign Money Exchange

Authors and Contributors

Authors

Melissa “Mel” Trumpower is the executive director of 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.

Melissa Bittner is the curriculum development and training manager for 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.

Contributors

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.

Katherine R. Hutt, APR, Fellow PRSA, is an award-winning communicator with 30 years’ experience helping non-profits, government agencies, entrepreneurs, and businesses tell their stories. She is Accredited in Public Relations with the Public Relations Society of America and a member of the PRSA College of Fellows. She serves as BBB national spokesperson and works closely with BBB communications professionals across North America to deliver timely and useful information to consumers on a variety of topics related to marketplace trust.

Amy Gwiazdowski is the director of internal strategic communications for the Council of Better Business Bureaus. Before joining CBBB, she was the communications director for a business trade association for companies with employee stock ownership plans (ESOPs) in Washington, DC. Previously, she spent a few years working for a publishing industry trade association, where she focused on First Amendment and copyright issues.





3033 Wilson Boulevard, Suite 600
Arlington, VA 22201

Institute@Council.BBB.org

BBB.org/RiskReport