INSTITUTE for MARKETPLACE TRUST

BBB

2021

BBB Scam Tracker℠ RISK REPORT

Cryptocurrency scams signal new marketplace risks

INSTITUTE for MARKETPLACE TRUST

BBB SM

2021

BBB Scam Tracker℠
RISK REPORT

Cryptocurrency scams signal new marketplace risks

Table of Contents

Introduction

The BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the Better Business Bureau® (BBB®), is pleased to present the *2021 BBB Scam Tracker Risk Report*. This annual report uses data submitted by individuals and businesses to BBB Scam Tracker℠ (BBB.org/ScamTracker) to shed light on how scams are perpetrated, who is being targeted, which scams have the greatest impact, and much more. Highlights of the 2021 report are provided in Figure 3.

This report is a critical part of our ongoing work to share timely data and analysis to support the efforts of all who are engaged in combating marketplace scams. Scams undermine trust in the marketplace, distort the level playing field, and siphon money from legitimate transactions that could benefit both businesses and consumers, thus impeding economic growth. A healthy marketplace requires empowered and aware consumers and principled businesses that are proactively working to stop scammers and honor trustworthy relationships.

Prevention is critical in our effort to reduce the impact of scams on consumers and businesses. Our risk report findings enable BBB Institute to develop needed consumer educational programs and resources. These resources are delivered digitally and in person, leveraging the expansive network of BBBs serving communities across North America.

Stopping scammers requires a multisector effort by government agencies and law enforcement, not-for-profits, the media, and the business community. BBB Institute shares its data with partners combating fraud in the marketplace. We work with leaders in business, law enforcement, and government to determine the best ways to stop scammers, and we partner with corporate partners and like-minded organizations to better allocate resources to tackle the problem, determine which prevention tactics are working, and then evolve those tactics as needed.

BBB Scam Tracker

The *BBB Scam Tracker Risk Report* is possible thanks to data from BBB Scam Tracker, an online platform that enables consumers and businesses to report attempted or successful acts of fraud they've experienced. These instances of fraud are reviewed and posted for the public, empowering others to identify scams and avoid losing money. In 2022, BBB Institute will launch a newly designed BBB Scam Tracker platform (more detail about the project is available on page 35).

BBB Scam Tracker's impact goes far beyond the tool itself. By monitoring real-time reports and overall trends, BBB, with local and network media partners, warns the public so as to reduce the impact of scammers.

More than 1.6 million people visited the platform in 2021[1], with 49.3% reporting that they sought to determine if they were experiencing a scam and 22.9% of those visitors reporting that BBB Scam Tracker helped them avoid losing money to a scammer[2]; we estimate BBB Scam Tracker helped people save $31.4 million in 2021 alone (Figure 1).

Our survey research also found that 98.1% of visitors to BBB Scam Tracker sought to warn others about a scam and 90.9% hoped to bring justice to the perpetrator.[2] We extend our thanks to the more than 276,000 citizen heroes who chose to speak out by reporting scams to BBB Scam Tracker to help others avoid losing money.

FIGURE 1 **2021 BBB Scam Tracker impact**

1,643,665

Unique visitors to BBB Scam Tracker

49.3%

Visited BBB Scam Tracker to determine whether they were experiencing a scam

About 1 of every 5 visitors

(22.9%) seeking to determine whether they were experiencing a scam said BBB Scam Tracker helped them avoiding losing money

$169

Median $ saved

$31,360,459

Estimated direct impact

[1] Adobe Analytics.

[2] Survey with 2,628 visitors to BBB Scam Tracker conducted in January 2022.

2021 overview

The data and insights gleaned via BBB Scam Tracker reports enable us to better understand the impact of scams being perpetrated in the marketplace. This report explores differences in risk borne by specific subsets of the population. In 2021, more than 46,000 scams were published via BBB Scam Tracker, a slight decrease (0.9%) from 2020. Scam reports submitted by businesses and individuals across North America are classified into 28 consumer scam types, 13 business scam types, and an "other" category, which represented 5.7% of all consumer reports (Appendix A). Data collected includes a description of the scam, the dollar value of any loss, and information about the means of contact and method of payment. Optional demographic data (age, gender, and postal code) about the person targeted by the scam along with military and/or student status were also reported via the BBB Scam Tracker platform. See Appendix B and Appendix C for detailed data by scam type.

One positive finding from this year's report is that susceptibility (the percentage of consumers who reported losing money when exposed to a scam) decreased for the first time since 2017, dropping 8.4% from 46.7% in 2020 to 42.8% in 2021 (Figure 2). It is concerning, however, that reported median dollar loss rose 47.0%, rebounding from an all-time low of $115 in 2020 to $169 in 2021.

With a continued increase in online shopping, remote work, and general online and social media browsing in 2021, it's not surprising that more scams were perpetrated online and yielded the highest likelihood of financial loss. Similar to 2020, the top three contact methods in 2021 that resulted in a reported monetary loss were website, social media, and email. Despite a slight drop in exposure and susceptibility, online purchase scams remained the riskiest scam in 2021. This scam type had the highest exposure of any scam type, comprising more than one-third of all scam types reported to BBB Scam Tracker, with almost 75% of people reporting a monetary loss when targeted by an online purchase scam.

Cryptocurrency scams rose to the second riskiest scam type in 2021 due to a reported increase in both exposure and susceptibility. Although cryptocurrency scams made up only 1.9% of the scams reported to BBB Scam Tracker, the median dollar loss was $1,200, much higher than the overall median dollar loss of $169. More than 66% of people reported losing money when targeted by this scam type.

This year, we also included the top scams reported by businesses. About 3.5% of all reports to BBB Scam Tracker in 2021 were for scams targeting a business (see Figure 17).[3] When targeted by a scam,

[3] Due to the self-reported nature of the scams, we estimate that 3.5% of total reports were related to scams targeting businesses.

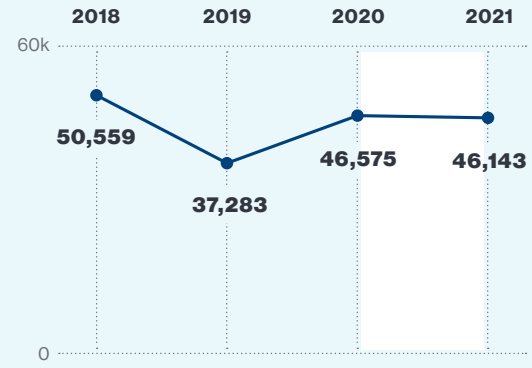
businesses reported losing money 21.7% of the time, significantly lower than the overall susceptibility for consumers (42.8%). However, the median dollar loss for businesses was higher ($245) than for consumers ($169). More information about business scams can be found on page 29.

FIGURE 2 **Snapshot of risk (2018–2021)**

EXPOSURE

Number of scam reports

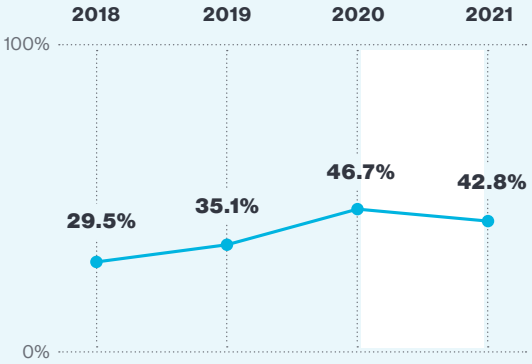
▼ **0.9%**
from 2020



SUSCEPTIBILITY

Percent of reports that included dollar loss

▼ **8.4%**
from 2020



MONETARY LOSS

Median reported dollar loss

▲ **47.0%**
from 2020

FIGURE 3

2021 Scam Tracker Risk Report
HIGHLIGHTS

SCAMS REPORTED **46,143**
DOWN 0.9%

LIKELIHOOD OF LOSS **42.8%**
DOWN 8.4%

MEDIAN $ LOSS **$169**
UP 47.0%

TOP 3 RISKIEST SCAMS REPORTED

BY CONSUMERS

1. Online purchase
2. Cryptocurrency
3. Employment

BY BUSINESSES

1. Fake invoice/ supplier bill
2. Bank/credit card company imposter
3. Worthless problem-solving service

ONLINE SCAMS CONTINUE TO DOMINATE

More than one third

(37.4%) of all scams reported in 2021 were **online purchase scams.**

59.8%

reported **shopping online** more this year as the pandemic continued.

46.4%

reported spending more time **browsing social media.**

Almost 3 out of every 4

(74.9%) of those targeted by online purchase scams **reported losing money.**

Online scams

were more likely to result in a reported monetary loss than those perpetrated in person or via phone.

2021 CHANGES IN SCAM RISK

- **Cryptocurrency scams** rose from seventh to **second riskiest.**
- **Amazon** rose to the **number one brand most impersonated** by scammers.
- **About the same percentage of people reported losing time** as reported losing money after being targeted by a scam.
- **Moving scams** were the scam type with the **highest reported susceptibility.**
- **Foreign money exchange scams** were the scam type with the **highest monetary loss.**
- **Investment scams** rose from the tenth to the **fifth riskiest scams for all ages.**

BBB Risk Index: A three-dimensional approach to measuring scam risk

To better understand which scam types pose the highest risk, we assessed scams based on three factors: exposure, susceptibility, and monetary loss. This unique formula is the BBB Risk Index (Figure 4). By combining these three factors, we gain a meaningful understanding of scam risk that goes beyond the volume of reports received, enabling BBB and its partners to better target scam prevention outreach.

Risk cannot be determined by viewing just one of these factors in isolation. For example, scams that occur in high volumes typically target as many people as possible but yield a lower likelihood of loss and/or monetary loss. In comparison, scams with a "high-touch" approach often reach fewer individuals, but those exposed individuals are often more likely to lose money and to lose more money.

FIGURE 4 **BBB Risk Index**

The formula for calculating the BBB Risk Index for a given scam in a given population is

Exposure ✖ Susceptibility ✖ (Median Loss / Overall Median Loss) x 1,000.

BBB RISK INDEX

EXPOSURE
is a measure of the prevalence of a scam type, calculated as the percentage of a particular scam type as part of the total scams reported.

✖

SUSCEPTIBILITY
is a measure of the likelihood of losing money when exposed to a scam type, calculated as the percentage of all reports that reported a monetary loss.

✖

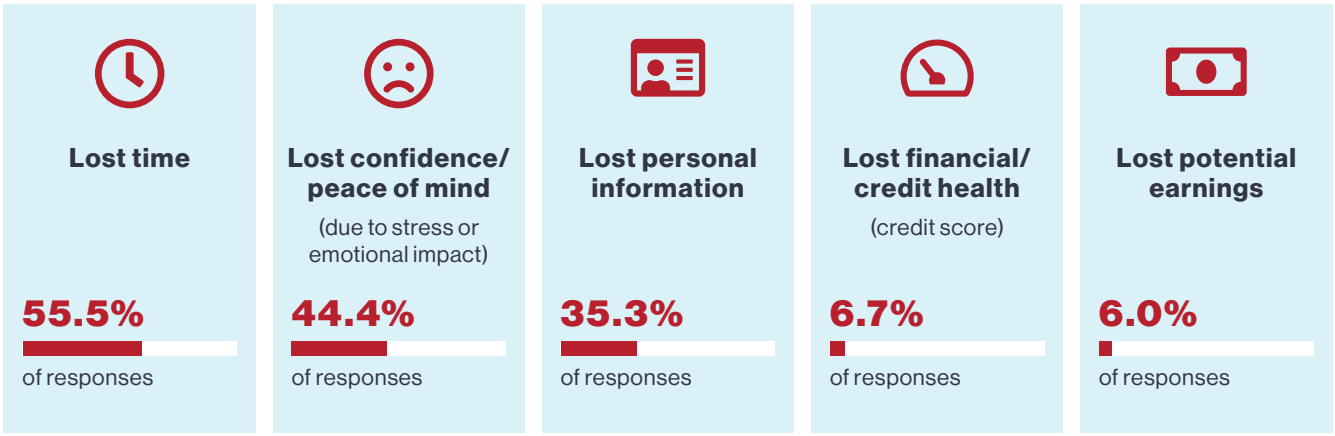
MONETARY LOSS
is calculated as the median dollar amount of losses reported for a particular scam type, excluding reports where no loss occurred.

The BBB Risk Index does not factor in the emotional and psychological harm scams can inflict or the damage done in diminishing trust in the marketplace due to those perpetrating fraud. Our survey research[4] explored the non-financial impacts of scams (Figure 5). More than 44% reported losing confidence or peace of mind because of the emotional impact of being targeted by a scam. Another interesting finding: about the same percentage of people (55.5%) reported losing time as reported losing money after being targeted by a scam.

About the same percentage of people reported losing time as reported losing money after being targeted by a scam.

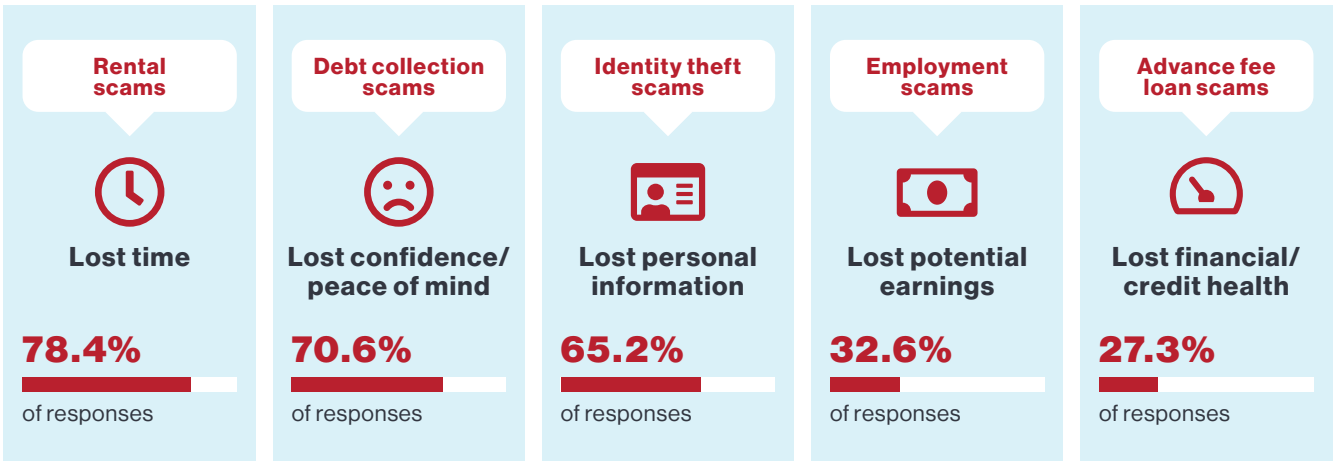
[4] A survey was distributed to those who submitted a scam to BBB Scam Tracker in 2021; 5,258 respondents completed the survey.

FIGURE 5 **Non-financial impacts of being targeted by a scam**



We sought to better understand which scam types were most often reported as resulting in non-financial impacts (Figure 6).

FIGURE 6 **Top scam types with reported non-financial impacts and monetary loss**



Note: Includes only scams reported by those reporting a monetary loss and scams that targeted them as an individual.

Top scams reported by consumers in 2021

Based on the BBB Risk Index and reports submitted to BBB Scam Tracker in 2021, the 10 riskiest scams (Table 1) pose the most significant risks to consumers; the list changed slightly with some notable shifts from 2020.

Online purchase scams made up more than a third of all scams reported in 2021 and cryptocurrency scams were the second riskiest scam.

Not surprisingly, online purchase scams[5] were the riskiest scam type for the second year in a row with people continuing to adjust to life with COVID-19. According to our survey research, 59.8% of respondents shopped more online in 2021 and 46.4% spent more time browsing online (including social media). Online purchase scams made up 37.4% of all scams reported to BBB Scam Tracker in 2021, with 74.9% reporting a monetary loss.

Cryptocurrency scams were the second riskiest scam in 2021, rising from seventh riskiest in 2020. Although cryptocurrency scams made up only 1.9% of the scams reported to BBB Scam Tracker in 2021, the median dollar loss was $1,200, much higher than the overall median dollar loss of $169. More than 66% of people reported losing money when targeted by this scam type.

Employment scams have been in the top three riskiest scams since we began publishing the *BBB Scam Tracker Risk Report* in 2016. In 2021, employment scams dropped from second riskiest to third. The susceptibility and median dollar loss of this scam type dropped slightly, while the number of reported scams increased from 7.1% in 2020 to 7.8% in 2021.

Other notable changes to the top 10 list include the rise of government grant scams to the eighth riskiest in 2021, up from the 13th spot in 2020 due to a rise in median dollar loss (up from $800 in 2020 to $1,000 in 2021) and susceptibility (up from 15.9% in 2020 to 19.5% in 2021). Romance scams, however, dropped from sixth on the list in 2020 to the 14th slot in 2021 because of a drop in median dollar loss (down from $2,100 in 2020 to $900 in 2021) and susceptibility (down from 45.9% in 2020 to 36.6% in 2021).

[5] Additional information about online purchase scams can be found in the *2021 Online Purchase Scams Report*, published by BBB Institute for Marketplace Trust.

TABLE 1 10 riskiest consumer scams in 2021

RANK		SCAM TYPE	BBB RISK INDEX	EXPOSURE		SUSCEPTIBILITY		MEDIAN $ LOSS	
2021	2020			2021	2020	2021	2020	2021	2020
1	1	Online purchase	167.4	37.4%	38.3%	74.9%	78.8%	$101	$96
2	7	Cryptocurrency	90.6	1.9%	0.7%	66.2%	55.8%	$1,200	$1,200
3	2	Employment	63.0	7.8%	7.1%	15.1%	16.6%	$900	$967
4	5	Home improvement	45.2	1.4%	0.7%	59.1%	58.7%	$955	$1,193
5	10	Investment	29.9	0.8%	0.6%	56.9%	67.2%	$1,100	$948
6	3	Fake check/ money order	27.1	2.1%	2.7%	14.8%	16.6%	$1,475	$1,679
7	4	Advance fee loan	25.9	1.8%	1.6%	40.6%	47.1%	$609	$745
8	13	Government grant	24.8	2.2%	2.0%	19.5%	15.9%	$1,000	$800
9	8	Tech support	22.0	3.1%	3.1%	24.3%	28.2%	$500	$499
10	9	Travel/vacation/ timeshare	20.3	0.9%	0.7%	56.5%	44.9%	$700	$1,300

Online purchase scams remained riskiest in 2021

Online purchase scams made up more than one-third of scams reported to BBB Scam Tracker in 2021. About 75% reported losing money when targeted by this scam type. As a result, it ranked as the #1 riskiest scam for the second year in a row. Puppy scams continued to top the list of products most used to perpetrate online purchase scams.

The following scam report was submitted by a woman, age 25-34, from Illinois:

> We reached out to what seemed like a legitimate dog breeder to purchase a puppy. Transaction for puppy went through, fake Bill of Sale was produced. Red flags went off when the shipping company the "breeder" uses said they charge $1,380 for shipping but refund $1,350 once the puppy is delivered to us. Seemed odd that including airfare, it would only cost $30 to ship him... started doing reversed image searches and scam searches and the shipping company came up as a reported scam, but not the fake "breeders" themselves. I want to make sure no more people get taken advantage of."

TIPS FOR AVOIDING ONLINE PURCHASE SCAMS

- **Be very wary of purchasing a pet online.**
- **Never use an online payment system to pay somebody you don't know.**
- **Search BBB Scam Tracker to see if another person has reported the person or business as a scammer.**

Cryptocurrency scams riskier in 2021

Cryptocurrency scams rose from seventh riskiest in 2020 to the second riskiest scam in 2021. We received many reports of people being targeted on a variety of social media platforms by scammers offering to help them invest in bitcoin.

The following scam report was submitted by a student, age 25-34, from Indiana:

> They hacked my friend's Instagram account and made it seem like they would be helping her invest money. So they tricked her, which tricked me. They had her post a video saying she got $10,000 after investing $500 in less than an hour. So they convince you to transfer money to cashapp and then make it bitcoin to which you then send it off to them. They have you sign up for their website to see the money that "accumulated" to $10,000. But what they try to do after that is have you give this processing fee of $1,500 to put your application of withdrawal, of the 10,000 dollars, to your account. And if you don't have that money they say their company will pull the cost if you make a video saying that you got $10,000 by investing $500 dollars in bitcoin through this firm and this agent on Instagram."

TIPS FOR AVOIDING CRYPTOCURRENCY SCAMS

- **Be very wary of anyone offering to make you quick money with little risk.**
- **Scammers can pretend to be your friend on social media by hacking into their accounts. Always check directly with the person before clicking a link or paying them money.**
- **If somebody claims to be a broker, check them on FINRA's BrokerCheck tool.**
- **Never use an online payment system to pay somebody you don't know.**
- **Search BBB Scam Tracker to see if another person has reported the person or business as a scammer.**

Demographics

The collection of self-reported demographic data such as age, gender, and racial background enhances our ability to identify individuals who are most at risk and helps us better understand how the nature of risk varies across different subgroups of the population. We use this information to enhance how we target outreach and educational strategies. BBB creates content, resources, and programming aimed at empowering consumers and businesses alike to identify and avoid scams.

In 2021, all age groups reported a higher median loss in 2021, with people ages 65+ reporting a higher median loss than all other age groups.

Age

In 2021, when targeted by a scam, younger people reported losing money at higher rates than older people. All age groups reported a higher median loss in 2021, with people ages 65+ reporting a higher median loss ($200) than all other age groups (Figure 7). However, younger age groups had the next highest monetary loss, with ages 25–34 reporting a median dollar loss of $175 and ages 18–24 reporting a monetary loss of $170.

Table 2 highlights the three riskiest scams by age. Online purchase scams were the riskiest for all age groups in 2021. Cryptocurrency scams were the second riskiest for ages 25–64. Employment scams were second riskiest for ages 18–24 and third riskiest for ages 25–44 and 55–64. Interestingly, investment scams were third riskiest for ages 18–24 for the first time since we began publishing the risk report. The rise of cryptocurrency scams as the second riskiest overall in 2021 may play a role in the rise of investment scams as the third riskiest for this age group.

FIGURE 7

Exposure, susceptibility, and median dollar loss of all scam types by age

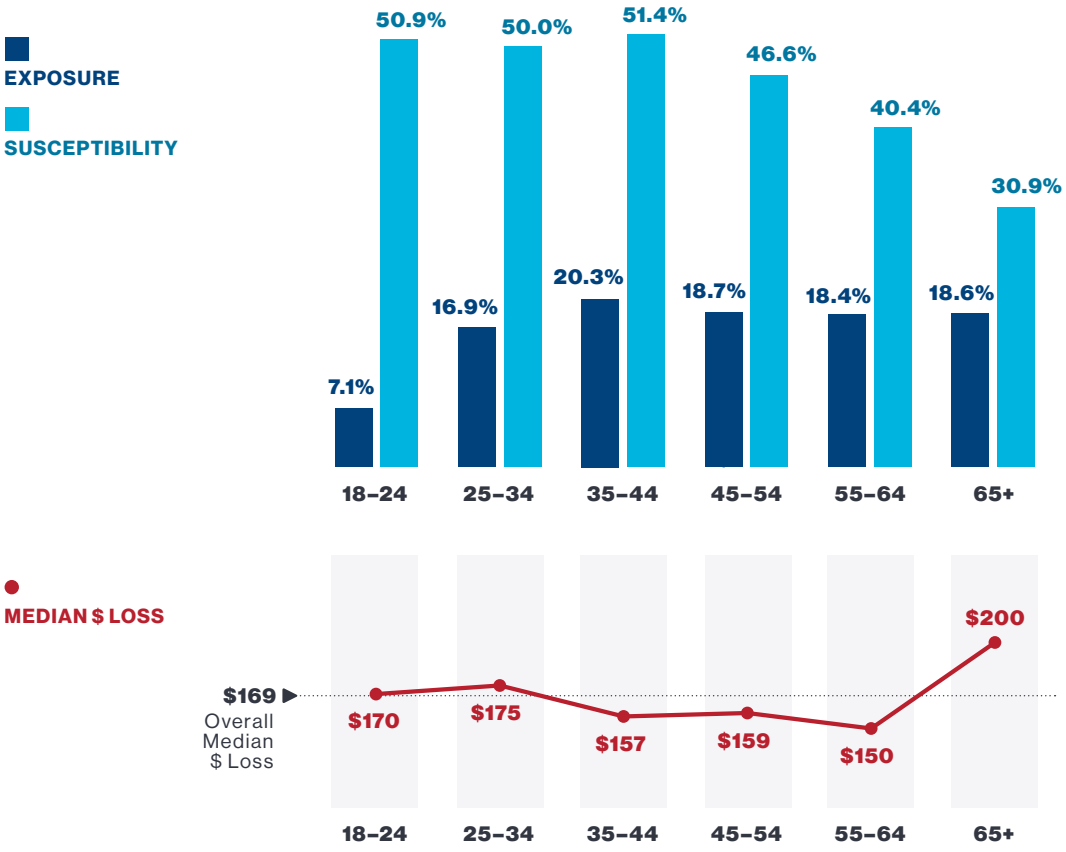


TABLE 2

Three riskiest scam types by age

	18–24	25–34	35–44	45–54	55–64	65+
1	Online purchase scams					
2	Employment scams	Cryptocurrency scams				Travel/ vacation/ timeshare scams
3	Investment scams	Employment scams	Employment scams	Home improvement scams	Employment scams	Tech support scams

Gender

Similar to previous years, more than two-thirds of reports to BBB Scam Tracker in 2021 were submitted by women; one-third of reports were submitted by men. Women were slightly more susceptible to losing money when exposed to a scam (43.6%) compared to men (42.9%) (Figure 8). The median dollar loss for women ($150) was significantly lower than that for men ($220). Online purchase scams were again the riskiest scams for men and women (Table 3). Cryptocurrency scams were the second riskiest for men and the third riskiest for women.

FIGURE 8 Exposure, susceptibility, and median dollar loss by gender

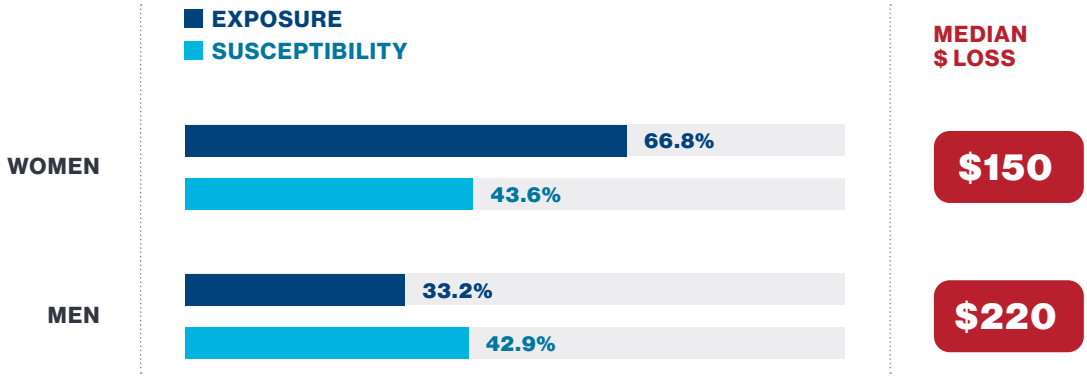


TABLE 3 Three riskiest scam types by gender

	WOMEN	MEN
1	Online purchase scams	
2	Employment scams	Cryptocurrency scams
3	Cryptocurrency scams	Home improvement scams

Scam delivery and payment methods

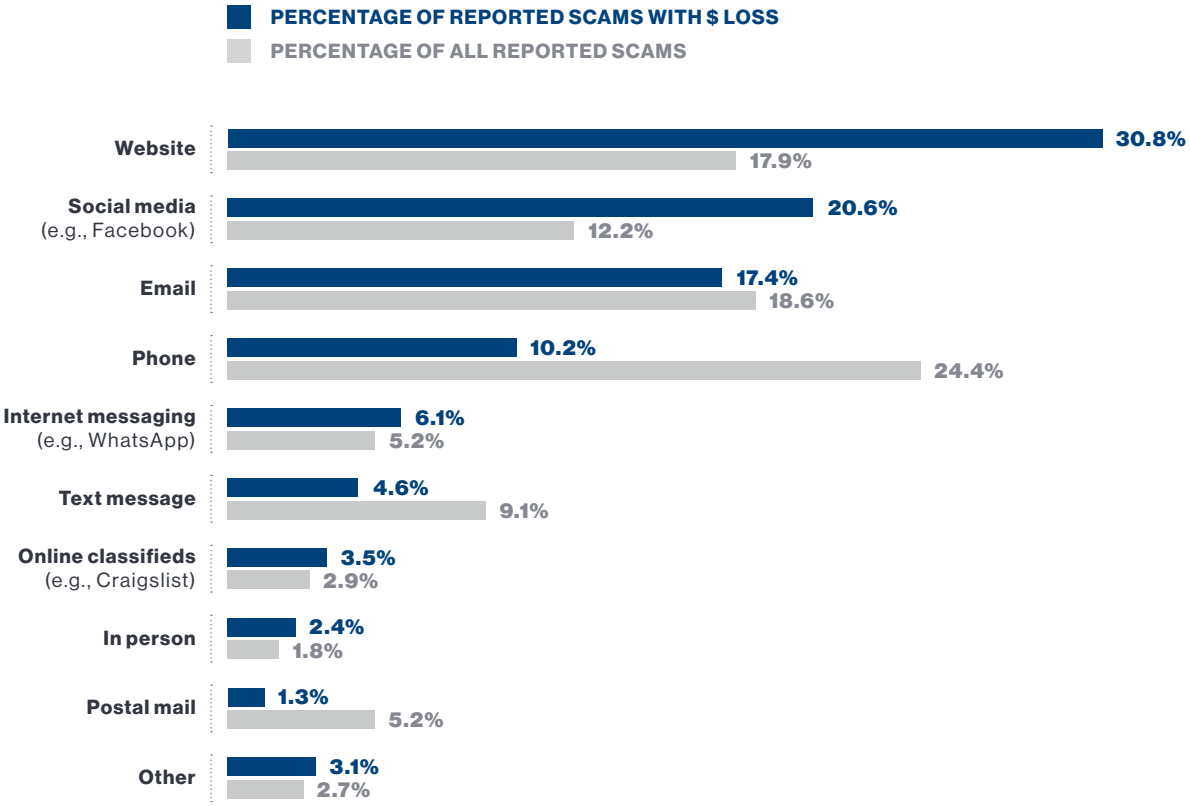
With a continued increase in online shopping, remote work, and general online browsing in 2021, it's not surprising that more scams were perpetrated online and yielded the highest reported financial loss. Similar to 2020, the top three contact methods in 2021 resulting in a reported monetary loss were website, social media, and email (Figure 9). Internet messaging rose slightly this year, up from 5.3% in 2020 to 6.1% in 2021. It's interesting to note that while in-person scams dropped significantly from 2019 (3.3%) to 2020 (1.5%), they rose 60% to 2.4% in 2021.

Phone continues to be the most common contact method reported to BBB Scam Tracker (24.4%), followed by email (18.6%) and website (17.9%) (Figure 9). Though fewer people reported losing money when targeted by phone (17.9%) than those targeted by website (73.7%) and social media (72.0%), the median dollar loss for scams perpetrated by phone ($573) was higher than website ($100) and social media ($90). Scams perpetrated via text message had a reported median dollar loss of $630 with 21.4% reporting they lost money when targeted. Scams perpetrated via online means were more prevalent overall than other delivery methods (56.8%), with a higher percentage of people losing money when targeted (78.4%) (Figure 10).

This year we examined the means of contact for monetary loss by age. Ages 65+ were less likely to report losing money when targeted via social media, email, and websites than other age groups, but they were more likely to report losing money when targeted by phone, Internet messaging, and online classifieds (Figure 11).

FIGURE 9

Percent of scams reported with monetary loss compared with total scams reported by means of contact



Susceptibility and monetary loss by means of contact

MEANS OF CONTACT	SUSCEPTIBILITY	MEDIAN $ LOSS
Website	73.7%	$100
Social media (e.g., Facebook)	72.0%	$90
Email	40.0%	$239
Phone	17.9%	$573
Internet messaging (e.g., WhatsApp)	50.7%	$436
Text message	21.4%	$630
Online classifieds (e.g., Craigslist)	52.3%	$238
In person	56.6%	$700
Postal mail	10.3%	$150
Other	48.3%	$189

FIGURE 10

Percent of scams reported with monetary loss compared with total reported scams by means of contact

Online
(includes website, social media, email, internet messaging, and online classifieds)

56.8%
of all scams reported

78.4%
of all scams reported with a $ loss

Phone
(includes phone and text messaging)

33.5%
of all scams reported

14.8%
of all scams reported with a $ loss

In person
(includes in person and postal mail)

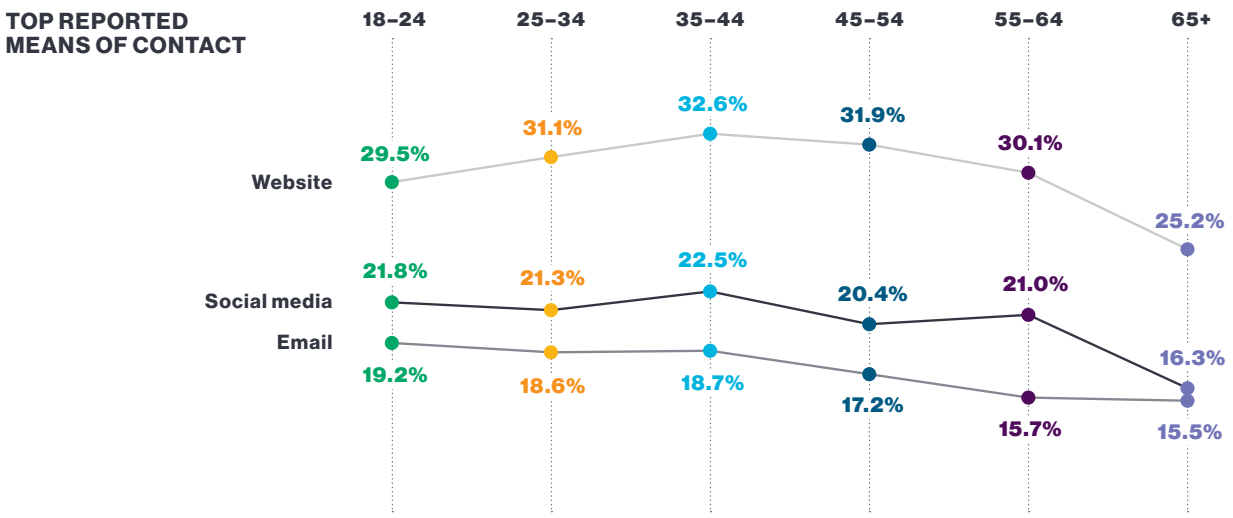
7.0%
of all scams reported

3.7%
of all scams reported with a $ loss

Note: Percentage of all scams and scams with a $ loss do not add up to 100% because the "other" category was not included.

FIGURE 11

Percent of scam reports resulting in monetary loss by means of contact and age

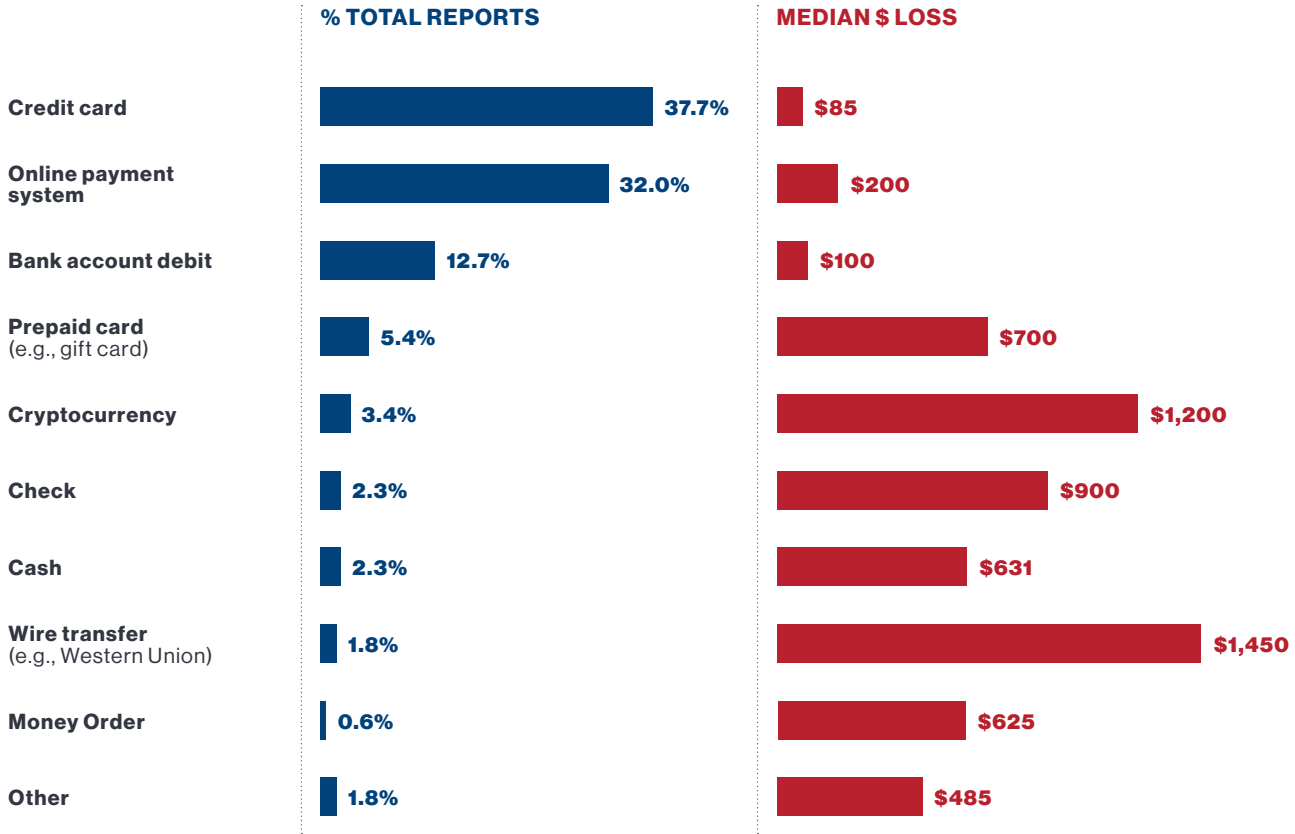


OTHER REPORTED MEANS OF CONTACT	18-24	25–34	35–44	45–54	55–64	65+
Phone	8.9%	9.4%	9.0%	9.4%	10.0%	15.9%
Internet messaging (e.g., WhatsApp)	5.8%	6.1%	4.8%	5.7%	6.7%	8.9%
Text message	4.9%	4.2%	4.1%	5.2%	5.6%	3.9%
Online classifieds	2.6%	2.6%	2.6%	4.2%	4.5%	4.3%
In person	3.1%	2.7%	2.5%	2.2%	2.1%	2.4%
Postal mail	1.5%	1.3%	1.1%	1.0%	0.9%	2.0%
Other	2.7%	2.7%	2.1%	2.8%	3.4%	5.6%

Payment made via cryptocurrency that resulted in a monetary loss more than doubled from 2020.

Credit cards (37.7%) remained the top reported payment method with a monetary loss in 2021 (Figure 12). Online payment systems were the second most common payment type with a dollar loss, up slightly from 31.2% in 2020 to 32.0% in 2021. Another significant finding in this year's report is that payment made via cryptocurrency that resulted in a monetary loss more than doubled from 2020 (1.5%) to 3.4% in 2021. The payment methods with the highest median dollar loss were wire transfer ($1,450), cryptocurrency ($1,200), check ($900), and prepaid card ($700).

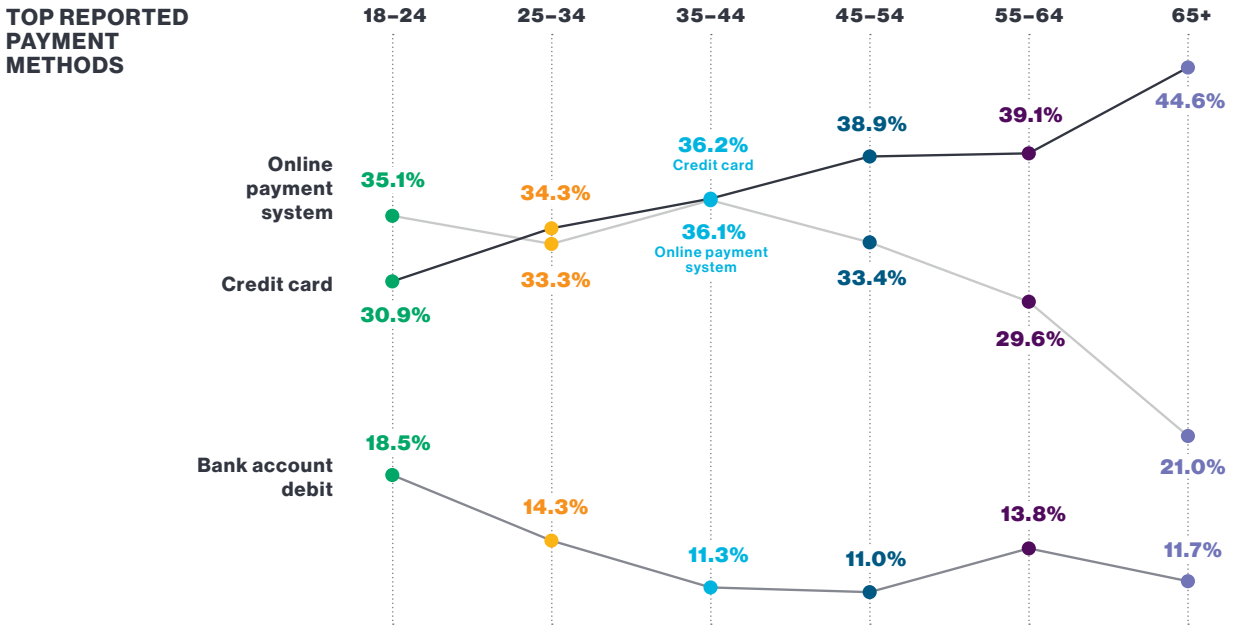
FIGURE 12 **Percent of total scam reports resulting in monetary loss by payment method**



When broken out by age, younger ages reported more instances of losing money via online payment system, bank account debit, and cryptocurrency (Figure 13). Older adults reported more instances of losing money via prepaid cards, credit card, and check.

FIGURE 13

Percent of scam reports resulting in monetary loss by payment method and age



OTHER REPORTED PAYMENT METHODS	18-24	25–34	35–44	45–54	55–64	65+
Prepaid card	4.0%	4.0%	4.1%	5.9%	6.5%	8.8%
Cryptocurrency	3.0%	5.5%	4.1%	3.3%	2.3%	0.9%
Cash	2.7%	2.8%	2.2%	1.7%	2.2%	2.9%
Check	1.3%	1.6%	2.0%	2.2%	2.2%	5.3%
Wire transfer (e.g., Western Union)	1.9%	1.7%	1.5%	1.6%	2.0%	2.3%
Money order	0.4%	0.4%	0.6%	0.6%	0.9%	0.9%
Other	2.2%	2.1%	1.9%	1.4%	1.4%	1.6%

Impact on specific audiences

Canadian consumers

In 2021, Canadian consumers reported 1,687 scam reports to BBB Scam Tracker (3.7% of total reports). The median reported loss was $250 CAD in 2021, which is an increase from $205 CAD in 2020. Susceptibility decreased slightly from 46.3% in 2020 to 45.1% in 2021. These trends—an increase in median dollar loss with a decrease in susceptibility—mirror the overall findings from all BBB Scam Tracker submissions, which include scams reported by U.S. consumers.

The riskiest scam type reported by Canadians in 2021 was cryptocurrency scams.

The riskiest scam type reported by Canadians in 2021 was cryptocurrency scams, due to the high susceptibility (69.6%) and a median dollar loss of $1,500 CAD (Table 4). Advance fee loan scams fell from the riskiest scam reported by Canadians in 2020 to the second riskiest in 2021, with a susceptibility of 57.7% and a median dollar loss of $1,000 CAD. The third riskiest scam type reported in Canada was online purchase scams, again making up almost a third of all scams reported by Canadians. Notably, phishing scams rose from the seventh riskiest scam in 2020 to the fifth riskiest in 2021. More information about scams reported by Canadians can be found in the *2021 BBB Scam Tracker Canadian Risk Report*.

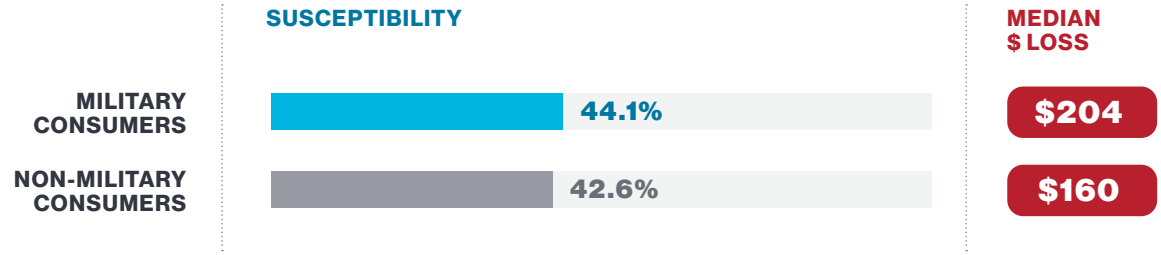
TABLE 4 **Top 3 riskiest scams in Canada**

RANK	SCAM TYPE	BBB RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN $ LOSS
1	Cryptocurrency	195.6	4.7%	69.6%	$1,500 CAD
2	Advance fee loan	142.3	6.2%	57.7%	$1,000 CAD
3	Online purchase	119.0	32.5%	73.0%	$125 CAD

Military families and veterans

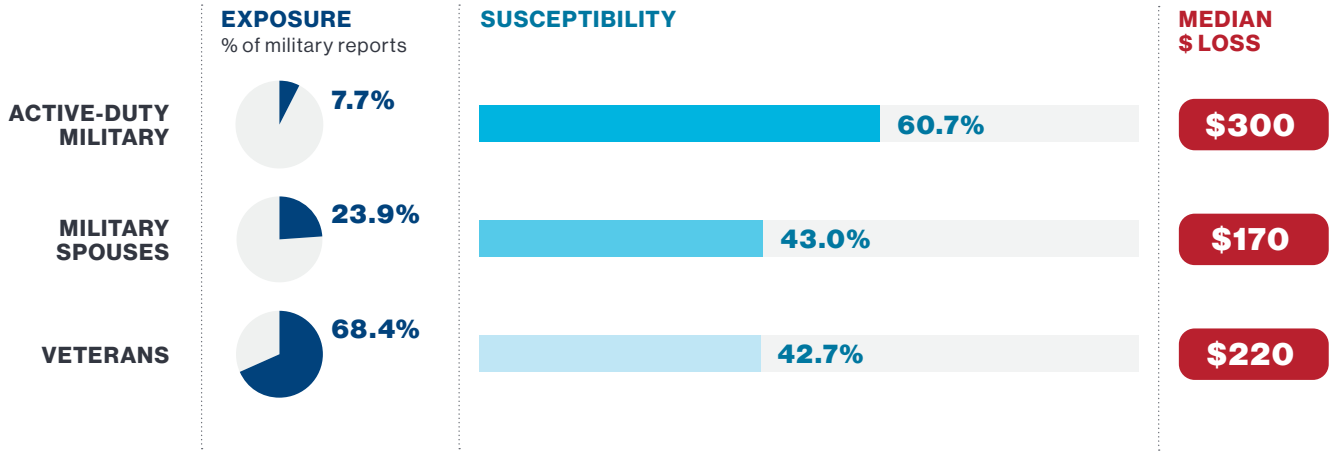
Over the years, our findings have suggested the military community is at an increased risk of losing money to scams. Individuals who self-identified as being active-duty military personnel, spouses, or veterans represented 10% of reports submitted to BBB Scam Tracker in 2021. Military consumers consistently report higher median financial losses than non-military consumers (Figure 14). In 2021, military consumers also reported higher rates of losing money when targeted by a scam than non-military consumers.

FIGURE 14 **Susceptibility and median $ loss reported by military families and veterans versus non-military**



In 2021, active-duty military reported losing significantly more money ($300) than military spouses ($170) or veterans ($220). While the percentages of military spouses (43.0%) and veterans (42.7%) who reported losing money when exposed to a scam were nearly identical to the percentage of the general population (42.8%) reporting monetary loss, the susceptibility of active-duty military (60.7%) was about 42% higher than the overall population's susceptibility (Figure 15).

FIGURE 15 **Exposure, susceptibility, and median $ loss reported by military families and veterans**



The BBB Risk Index was applied to identify the three riskiest scams for military spouses and veterans (Table 5). Online purchase scams were the riskiest for both military spouses and veterans in 2021 with employment scams being the second riskiest scam for both. Phishing scams were the third riskiest for military spouses, and home improvement scams were the third riskiest for veterans. Reports submitted by active-duty service members were spread out among the almost 30 scam types, with only online purchase scams having a significant number of scam records.

TABLE 5

Three riskiest scam types for military spouses and veterans compared with non-military consumers

	MILITARY SPOUSES	VETERANS	NON-MILITARY
1	Online purchase scams		
2	Employment scams		Cryptocurrency scams
3	Phishing scams	Home improvement scams	Employment scams

Students

Individuals who self-identified as students represented 8.3% of reports submitted to BBB Scam Tracker in 2021. Students continue to be more vulnerable when exposed to a scam: 51.5% of students reported a loss when exposed to a scam, which is significantly higher than susceptibility reported by non-students, at 42.0% (Figure 16). Students in 2021 reported roughly the same level of financial losses from scams ($170) as non-students ($169). Table 6 includes the riskiest scams for students. Online purchase scams were riskiest for students, with cryptocurrency and fake check/money order scams ranking second and third, respectively.

FIGURE 16 **Susceptibility and median $ loss reported by students versus non-students**

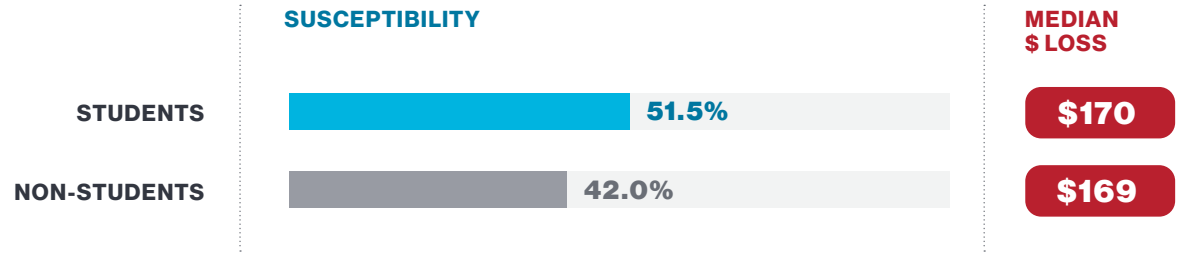


TABLE 6 **Three riskiest scam types for students compared with non-students**

	STUDENTS	NON-STUDENTS
1	Online purchase scams	
2	Cryptocurrency scams	
3	Fake check/ money order scams	Employment scams

Impersonated organizations/brands

"Impersonation" is one of the most common tactics fraudsters use to perpetrate scams. By pretending to be well-known and trusted companies, government agencies, and organizations, scammers can better manipulate their targets.

Amazon became the most impersonated organization reported to BBB Scam Tracker.

In 2021, Amazon became the most impersonated organization reported to BBB Scam Tracker, with twice the number of reports as the second most impersonated brand, the Social Security Administration (Table 7). PayPal rose to the fourth most impersonated brand, according to our reports, up from the sixth most impersonated in 2020. Facebook rose to the tenth most reported impersonated brand, and the U.S. Postal Service ranked as the 11th most reported impersonated organization. According to reports submitted to BBB Scam Tracker, scammers also impersonated warranty companies (192 reports) and Powerball winner Manuel Franco (85 reports).

TABLE 7 Top 10 organizations/brands used for impersonation

RANK	BUSINESS NAME	SCAMS
1	Amazon	1,460
2	Social Security Administration	697
3	Publishers Clearing House	395
4	PayPal	181
5	Medicare	149
6	Microsoft	137
7	Apple	125
8	Walmart	118
9	Cash Advance/Advance America	95
10	Facebook	90

Scams reported by businesses

About 3.5% of all reports to BBB Scam Tracker in 2021 were for scams targeting a business (Figure 17).[6] When targeted by a scam, businesses reported losing money 21.7% of the time, a significantly lower susceptibility than the overall susceptibility of consumers (42.8%). However, the median dollar loss for businesses was higher ($245) than for consumers ($169).

The most reported business scams (highest exposure) were fake invoice/supplier bill, government agency imposter, and bank/credit card company imposter scams (Table 8).

Based on the BBB Risk Index, the top three riskiest scams reported by businesses were fake invoice/supplier bill, bank/credit card company imposter, and worthless problem-solving service scams (Table 8).

FIGURE 17

Exposure, susceptibility, and monetary loss resulting from scams reported by businesses

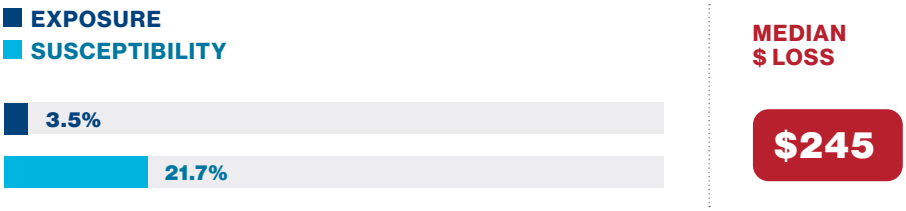


TABLE 8

Top three RISKIEST and MOST REPORTED scam types for businesses

	RISKIEST SCAMS FOR BUSINESSES	SCAMS MOST REPORTED BY BUSINESSES
1	Fake invoice/supplier bill	Fake invoice/supplier bill
2	Bank/credit card company imposter	Government agency imposter
3	Worthless problem-solving service	Bank/credit card company imposter

[6] Due to the self-reported nature of the scams, we estimate that 3.5% of total reports were related to scams targeting businesses.

Fake invoice/supplier bill scams target business employees

The riskiest and most prevalent scam type reported by businesses in 2021 were fake invoice/supplier bill scams. Scammers approach employees of the business to pay for products the business didn't order. Fake invoices/bills are submitted for office supplies, website or domain hosting services, directory listings, and more.

The following scam report was submitted by a business owner/manager from Texas:

> This company will call and try and get the warehouse, production, or operations manager. Then they send you a bunch of the cheapest tape you didn't order and try to bill your company for it. Unfortunately someone from my company fell for this scam a few years ago and they STILL call constantly from different numbers and iterations of their name, but the scam is the same every time. What kind of supply company doesn't have a website with a catalog? SCAMMERS, that's who."

TIPS FOR AVOIDING FAKE INVOICE/SUPPLIER BILL SCAMS

- **Take time to share information about scams targeting businesses with your employees.**
- **Make sure your business ordered the product/service.**
- **Do background research on the company before sending payment.**
- **Search BBB Scam Tracker to see if somebody has reported the person/fake business for scamming people.**

Lifestyle changes may impact susceptibility

Our survey research confirmed our suspicions that people continued making lifestyle changes during the second year of the global pandemic. This likely played a role in their exposure and susceptibility to scams (Figure 18). Those who reported shopping more online, relocated because of a shift in employment, purchased a pet, or were unable to keep up with their bills, were more likely to report losing money when targeted by a scam.

Self-reported cues and behaviors that helped people avoid losing money

Our team asked survey respondents to self-report how they handle certain situations (Figure 19). Those who reported being less likely to panic during a stressful situation were less likely to report losing money to scams than those who said they were likely to panic. Similarly, those who reported being more skeptical in dealing with new situations or persuasive offers were less likely to report losing money than those who said they were less likely to be skeptical. Those who reported experiencing significant financial distress during the past year were more likely to report losing money to scams compared to those who reported not experiencing financial distress.

FIGURE 18 **Survey respondents reported lifestyle changes resulting from COVID-19 in 2021.**

59.8%
I shop more online.

46.4%
I spend more time browsing online or on social media.

24.6%
I have been working from home more often.

21.2%
My employment status changed and/or I lost my job.

14.1%
I have been unable to keep up with my bills.

10.8%
I relocated/moved because of a job or other change in my life.

9.7%
I have children at home who are doing distance learning.

9.6%
I got a pet because I am home more often.

FIGURE 19 **Cues/behaviors survey respondents said helped them avoid losing money to a scam**

Though a significant number of respondents reported avoiding losing money to a scam because they "felt something wasn't right about the situation," when we combined the options, we found that the majority (~68%) of respondents who saved money identified at least two other cues in addition to trusting their gut. Following your gut appeared to be most protective when combined with another factor such as knowledge about scammer tactics and behaviors in general or researching the scam type or offer.

Following your gut appeared to be most protective when combined with another factor such as knowledge about scammer tactics and behaviors in general or researching the scam type or offer.

10 GENERAL TIPS
for avoiding a scam

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 or text messages.**

3 **Don't believe everything you see or read.**

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 **Take precautions when making online purchases.**

Don't shop on price alone. Scammers offer hard-to-find products at great prices.

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. Research the company first at BBB.org.

Avoid making quick purchases while browsing social media. Scammers advertise websites that offer great deals, but either don't deliver the product at all or deliver counterfeit products.

Do more research on those products you found via online search.

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.**

Learn more at BBB.org/AvoidScams

BBB Institute for Marketplace Trust

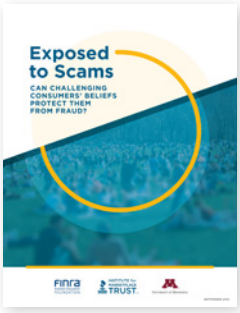
The *BBB Scam Tracker Risk Report* is published each year by the BBB Institute for Marketplace Trust (BBB Institute), the charitable arm of the Better Business Bureau. Our mission is to educate and protect consumers, establish best practices for businesses, and solve complex marketplace problems. Our consumer educational programs, which include a wide array of resources on fraud prevention and education, are delivered digitally and by BBBs serving communities across North America. Research is an integral component of our work, enabling us to incorporate the latest scammer trends in our consumer education resources and initiatives. You can find more information about BBB Institute and its programs at BBBMarketplaceTrust.org.

Recent BBB Institute research reports

2021 Online Purchase Scams Report

With online purchase scams ranking as the riskiest scam type for the second year in a row, BBB Institute used BBB Scam Tracker data and survey research to better understand the impact of this scam type, who is losing money, and how people can find trusted online sources to make better buying decisions.

Download at BBB.org/OnlinePurchaseScams2021



Exposed to Scams: Can Challenging Consumers' Beliefs Protect Them from Fraud?

A collaboration between BBB Institute, the FINRA Foundation, and the University of Minnesota, this report is based on in-depth, in-person interviews with 17 people and two scammers sharing their experiences with fraud attempts. The report explores four mental frames—or default ways of thinking about the world—that appeared to play a role in the way the interviewees perceived fraud attempts and whether they lost money to scams.

All BBB Institute research can be found on our website at BBBMarketplaceTrust.org.

Upgraded BBB Scam Tracker coming in 2022

Since it was launched in 2015, BBB Scam Tracker has enabled people to both report fraud and determine whether they were experiencing a scam so they could hang up the phone, delete a text message, or otherwise remove themselves from the situation. We estimate the platform helped consumers avoid losing about $31.4 million in 2021 alone. The data from BBB Scam Tracker is also shared with law enforcement and other partners working together to combat scams in the marketplace. We believe we can expand the impact of BBB Scam Tracker.

This year, BBB Institute is redesigning BBB Scam Tracker with generous support from Amazon and Capital One. The new platform will provide increased interaction capabilities and enable future enhancements based on consumer input. Once it is launched, BBB Institute will make continuous upgrades to meet the growing needs of consumers who lose money to scams, particularly demographic groups that are more susceptible to fraud.

The first stage of the new-and-improved BBB Scam Tracker is tentatively scheduled to go live in summer 2022.

Acknowledgments

BBB Scam Tracker utilizes the strength of the 110-year-old BBB brand to collect data from people who have been targeted by fraudsters. The program is made possible thanks to the dedicated, collaborative work of BBBs across North America; BBBs review consumer reports to eliminate those that do not appear to be actual scams, thus ensuring the best data possible.

We'd like to thank a team of BBB experts who provide guidance and input to BBB Institute regarding the BBB Scam Tracker program, including Warren King, president and CEO of the BBB Serving Western Pennsylvania; Jane Rupp, president and CEO of the BBB Serving Northern Nevada and Utah; Craig Turner, director of information systems of the BBB Serving Eastern & Southwest Missouri & Southern Illinois; Dené Joubert, investigations manager of the BBB Great West + Pacific; Jon Bell, the director of business relations of the BBB Serving Delaware; David Wheeler, vice president of innovation and development of the BBB Serving Central Florida; and Yolanda Moore, investigations director of the BBB Serving Western Pennsylvania.

We would also like to thank the International Association of Better Business Bureaus for its support of BBB Institute and the *2021 BBB Scam Tracker Risk Report.* Special thanks to Dr. Sean Xiangwen Lai, IABBB research and development specialist; Dr. Rubens Pessanha, MBA, PMP, SPHR, GPHR, SHRM-SCP, senior director, research & development, IABBB; and Matt Scandale, IABBB senior data analyst, for analyzing the data from BBB Scam Tracker for this report. We'd also like to thank IABBB Director of Communications Sandra Guile, IABBB Director of Brand Management Jody Thomas, and IABBB Deputy General Counsel Angel Isabell for providing their insights and input and helping us share these findings with the public.

Project team

Stacey Burns is the director of programs and communications for the BBB Institute for Marketplace Trust. Stacey worked for BBB of Southern Colorado for four and half years and has operated several social impact businesses in her career over the past two decades. She is the cofounder of the National Institute for Social Impact. Stacey has a bachelor's degree in psychology and English as well as a master's degree in counseling psychology, all from the University of Colorado.

Dr. Sean Xiangwen Lai is a research and development specialist at the International Association of Better Business Bureaus. Sean has experience in data gathering, processing, and data analysis and visualization and is currently finishing his PhD in physics at Georgetown University. He has passed two levels of Charter Financial Analyst (CFA) exams and is pursuing a CFA charter holder. He has a great passion for implementing statistics, programming, data analysis, finance, and marketing to decision making and innovation that have a positive impact on society. Sean speaks English, Mandarin, and Hokkien fluently, as well as some Japanese and Korean. His hobbies include all kinds of outdoor activities.

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

Melissa "Mel" Trumpower is the executive director of BBB Institute for Marketplace Trust. Mel has more than 25 years of nonprofit leadership experience working with a wide range of nonprofit organizations and trade associations. In addition to leading BBB Institute, Mel manages the BBB Scam Tracker program and is the coauthor of the *Online Purchase Scams Report* (2020 and 2021), the *BBB Scam Tracker Risk Report* (2017–2019), *Scams and Your Small Business* (2018), *Exposed to Scams* (2019 and 2021), the *Employment Scams Report* (2020), and *Building Better Together: The BBB Impact Report* (2021). Mel has a bachelor's degree from Cornell University and a master's degree from Johns Hopkins University.

APPENDIX A: GLOSSARY OF SCAM TYPES

Scams reported to BBB Scam Tracker this year are classified into 28 consumer scams and seven business-only scams. These classifications represent common scams reported to BBB and are informed by type classifications used by the Federal Trade Commission and the Internet Crime Complaint Center of the Federal Bureau of Investigation. Although scams vary widely, about 95 percent of all scams reported to BBB Scam Tracker can be classified into one of these general types.

The scam type definitions shaded in blue are **REPORTED ONLY BY BUSINESSES.**

ADVANCE FEE LOAN	A loan is guaranteed, but once the victim pays up-front charges such as taxes or a "processing fee," the loan never materializes.
BANK/CREDIT CARD COMPANY IMPOSTER	By impersonating a bank or credit card issuer, the scammer pretends to verify account information to get their targets to share credit card or banking information.
BUSINESS EMAIL COMPROMISE	Scammers gain access to a company's 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; however, they are typically of inferior quality. This can result in a life-threatening health or safety hazard when the counterfeit item is medication, a supplement, or an auto part.
COVID-19	Scammers seek to make money off the COVID-19 pandemic in some manner, such as by offering nonexistent or inferior products such as masks or cleaning supplies or any other scam type that uses the COVID-19 situation to steal money or personal information.
CREDIT CARD	Scammers impersonate a bank or other credit card issuer, pretending to verify account information to get a target's 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. The situations often 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 even though 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	Phony debt collectors harass their targets to get them to pay debts they don't owe.
EMPLOYMENT	Job applicants are led to believe they are applying for or have just been hired for a promising new job when instead they have given personal information via a fake application 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	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.

APPENDIX A: GLOSSARY OF SCAM TYPES

FAKE INVOICE/ SUPPLIER BILL	Employees pay for products that the business did not order or that don't even exist. Fake invoices are often submitted 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 experiencing a fabricated urgent or dire situation. The "loved one" invariably pleads for money to be sent immediately. Aided by personal details typically found on social media, imposters can offer very plausible stories to convince their targets.
FOREIGN MONEY EXCHANGE	The target receives an email from a foreign government's official, member of royalty, or a business owner offering a huge sum of money to help get money out of the scammer's country. The victim fronts costs for the transfer, believing they will be repaid.
GOVERNMENT AGENCY IMPOSTER	Scammers impersonating government agents threaten to suspend business licenses, impose fines, or even take legal action if the business doesn't pay taxes, renew government licenses or registrations, or pay other fees. Sometimes they trick businesses into buying workplace compliance posters that are available for free, or they may pressure them to pay up-front fees for a nonexistent business grant.
GOVERNMENT GRANT	Individuals are enticed by promises of free, guaranteed government grants requiring an up-front "processing fee." Other fees follow, but the promised grant never materializes.
HEALTHCARE, MEDICAID, AND MEDICARE	The scammer seeks to obtain the insured's health insurance, Medicaid, or Medicare information to submit fraudulent medical charges or for purposes of identity theft.
HOME IMPROVEMENT	Door-to-door solicitors offer quick, low-cost repairs and then either take payment without returning, do shoddy work, or "find" issues that dramatically raise the price. These types of schemes often occur after a major storm or natural disaster.
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	Scammers offer discounted pricing to move household items. The alleged movers may steal the items or hold them hostage from the customer, demanding additional funds to deliver them to the new location.
ONLINE PURCHASE	These scams typically involve the purchase of products and/or services where the transaction occurs via a website or other online means. Scammers use technology to offer attractive deals, but once the payment is made, no product or service is delivered. In some cases, fraudsters send low-quality or counterfeit products.
PHISHING/ SOCIAL ENGINEERING	In these schemes, scammers impersonating a trustworthy entity, such as a bank or mortgage company, employ communications to mislead recipients into providing personal information that the scammer will use to gain access to bank accounts or steal the recipient's identity. This type of scheme can also happen within the workplace as an email coming from the CEO, accounting, or other member of management seeking personal information.
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.

APPENDIX A: GLOSSARY OF SCAM TYPES

ROMANCE	An individual believing he/she is in a romantic relationship agrees to send money, personal and financial information, or items of value to the perpetrator.
SCHOLARSHIP	Victims, often students struggling with tuition costs, are promised 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/PRIZES	Victims are tricked 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	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 back taxes or sharing personal information.
TECH SUPPORT	Tech support scams start with a call or pop-up warning that alerts the target of a computer bug or other problem. Scammers posing as tech support employees from well-known tech companies hassle victims into paying for "support." If the victim allows remote access, malware may be installed.
TRAVEL/VACATION/ TIMESHARE	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	Imposters act as 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.
VANITY AWARD	The business receives a notice indicating that an employee or the business itself has won recognition for an achievement such as a "Best of Local Business Award." To claim their award, the "winner" must pay a fee.
WORTHLESS PROBLEM-SOLVING SERVICE	Sometimes scammers claim to be able to provide low-cost solutions to problems they know many businesses have. For example, they might claim they can repair the business's online reputation or provide quick relief if it's struggling with debt or back taxes, all for an up-front fee.
YELLOW PAGES/ DIRECTORY	Businesses are fooled 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 TYPE DATA TABLE, CONSUMER SCAMS

SCAM TYPE	RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN $ LOSS
Advance fee loan	25.9	1.8%	40.6%	$609
Charity	0.6	0.5%	20.0%	$100
Counterfeit product	12.3	3.5%	66.7%	$90
COVID-19	2.7	0.8%	14.8%	$400
Credit card	5.6	1.8%	38.0%	$139
Credit repair/debt relief	14.0	1.2%	32.7%	$600
Cryptocurrency	90.6	1.9%	66.2%	$1,200
Debt collection	6.1	3.0%	7.8%	$450
Employment	63.0	7.8%	15.1%	$900
Fake check/money order	27.1	2.1%	14.8%	$1,475
Family/friend emergency	4.5	0.4%	26.1%	$800
Foreign money exchange	5.1	0.1%	27.8%	$3,724
Government grant	24.8	2.2%	19.5%	$1,000
Healthcare/Medicaid/Medicare	2.7	1.4%	12.9%	$250
Home improvement	45.2	1.4%	59.1%	$955
Identity theft	6.2	1.9%	19.8%	$283
Investment	29.9	0.8%	56.9%	$1,100
Moving	3.7	0.9%	76.0%	$90
Online purchase	167.4	37.4%	74.9%	$101
Phishing/social engineering	17.6	11.9%	9.30%	$270
Rental	13.4	0.9%	49.5%	$504
Romance	12.5	0.6%	36.6%	$900
Sweepstakes/lottery/prizes	7.2	4.5%	13.3%	$200
Tax collection	0.6	0.2%	19.1%	$236
Tech support	22.0	3.1%	24.3%	$500
Travel/vacation/timeshare	20.3	0.9%	56.5%	$700
Utility	4.5	1.2%	12.3%	$500
Yellow Pages/directories	0.8	0.1%	29.4%	$550
Other	51.8	5.7%	37.2%	$400

APPENDIX C: Top 10 consumer scam types ranked by overall risk, exposure, susceptibility, and monetary loss

	BY RISK INDEX	BY EXPOSURE	BY SUSCEPTIBILITY	BY MEDIAN $ LOSS
1	Online purchase	Online purchase	Moving	Foreign money exchange
2	Cryptocurrency	Phishing	Online purchase	Fake check/ money order
3	Employment	Employment	Counterfeit product	Cryptocurrency
4	Home improvement	Sweepstakes/ lottery/prizes	Cryptocurrency	Investment
5	Investment	Counterfeit product	Home improvement	Government grant
6	Fake check/ money order	Tech support	Investment	Home improvement
7	Advance fee loan	Debt collection	Travel/vacation/ timeshare	Romance
8	Government grant	Government grant	Rental	Employment
9	Tech support	Fake check/ money order	Advance fee loan	Family/friend emergency
10	Travel/vacation/ timeshare	Cryptocurrency	Credit card	Travel/vacation/ timeshare

INSTITUTE for MARKETPLACE TRUST SM

Institute@IABBB.org

BBBMarketplaceTrust.org/RiskReport