



RESEARCH COLLABORATION SERIES

# New Insights into Demographic Groups More Vulnerable to Scams

University of Minnesota and the University of Southern California  
in collaboration with the BBB Institute for Marketplace Trust<sup>SM</sup>







## CONTENTS

### 03

#### Introduction

---

### 04

#### Reported Scams and the Impact of COVID-19

General Trends

Impact of COVID-19

Summary

Methodology

---

### 16

#### Prevention Tips for Avoiding Scams

---

### 18

#### Authors and Contributors

---

### 19

#### BBB® Resources

How to Collaborate  
with BBB on Research

Other Research by  
the BBB Institute

About BBB Institute

AN INTRODUCTION FROM  
BBB INSTITUTE FOR MARKETPLACE TRUST

# Fresh insights and perspectives regarding the ever-changing scam landscape are critical to efforts aimed at combatting fraud in the marketplace.

We are pleased to collaborate with researchers at the University of Minnesota and the University of Southern California to gain a broad perspective on data collected through the BBB Scam Tracker consumer reporting platform between 2017 and 2020. Dr. Linli Xu (University of Minnesota), Dr. Yi Zhu (University of Minnesota), and Dr. Anthony Dukes (University of Southern California) spent several months analyzing scam reports submitted by consumers to better understand the latest scam tactics being perpetrated in the marketplace. This report was created in collaboration with the BBB Institute for Marketplace Trust, the International Association of Better Business Bureau's research and development team, and the BBB serving Minnesota & North Dakota.

As we have found in our past research, scammers change their tactics often, taking advantage of events promoted in the media and emerging technologies. Effectively combatting fraud requires consistent new research to identify the latest scammer tactics. It also requires an understanding of which demographic groups are most vulnerable to specific types of fraud. This information enables BBB and our partners that have joined in the fight against fraud to more effectively target consumer education initiatives.

We are pleased to publish these findings, expanding on existing research with the goal of empowering consumers to protect themselves against fraud in the marketplace.





# Reported Scams and the Impact of COVID-19

An analysis of reported scams to BBB Scam Tracker<sup>SM</sup> indicated a number of trends. This report highlights the results from that analysis, with particular attention to the COVID-19 pandemic period.

## ANALYSIS CONDUCTED AND PREPARED BY

**Linli Xu**, University of Minnesota

**Yi Zhu**, University of Minnesota

**Anthony Dukes**, University of  
Southern California

## DATA COLLECTED

**Jan. 2017 – Sept. 2020**

## TOTAL REPORTED

**167,000+ Scams**

3% of which were reported from Canada

# General Trends

Reported here are the general trends in reported scams and victimization across the entire period. Victimization is defined as a reported scam indicating positive monetary loss. A majority of reported scams indicate that no money was lost. In fact, only 30% of all reports indicate actual victimization.

## REPORTED SCAMS

Attempts to scam through online purchases generate the most amount of scam reporting. As seen in the time series of Figure 1, scams involving online purchases are persistently the leading scam type reported, followed by phishing requests. Both of these scam types spiked in 2020, events we discuss in more detail later in this report.

FIGURE 1

*Time Trends of Selected Scam Types*

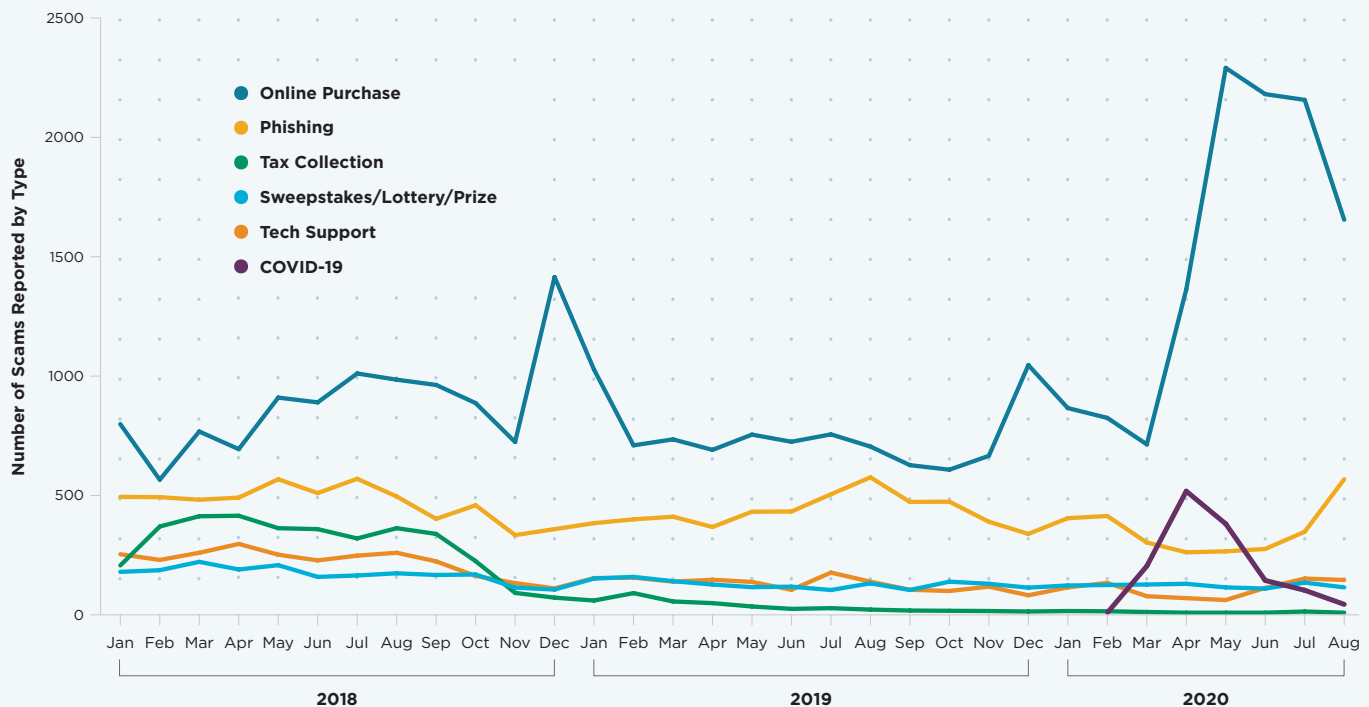


FIGURE 2

*Scam Type and Incidence of Victimization<sup>1</sup>*



## REPORTED VICTIMIZATION

We analyzed the factors that contribute to the incidence of victimization and the amount of victimization.

Two types of factors are considered:

1. We examined factors related to the scam itself, specifically scam type and means of contact.
2. We studied the impact of a victim's demographics. This analysis makes use of additional data from the U.S. Census on demographic averages for the zip code of the reported scam.

Figure 2 reports the relative impact of each scam type on the incidence of victimization.

For instance, phishing scams are less likely to result in monetary losses than scams related to romance and false claims of tech support. People in the sample are most vulnerable to losing money in moving and online purchase scams and least vulnerable in tax collection scams.

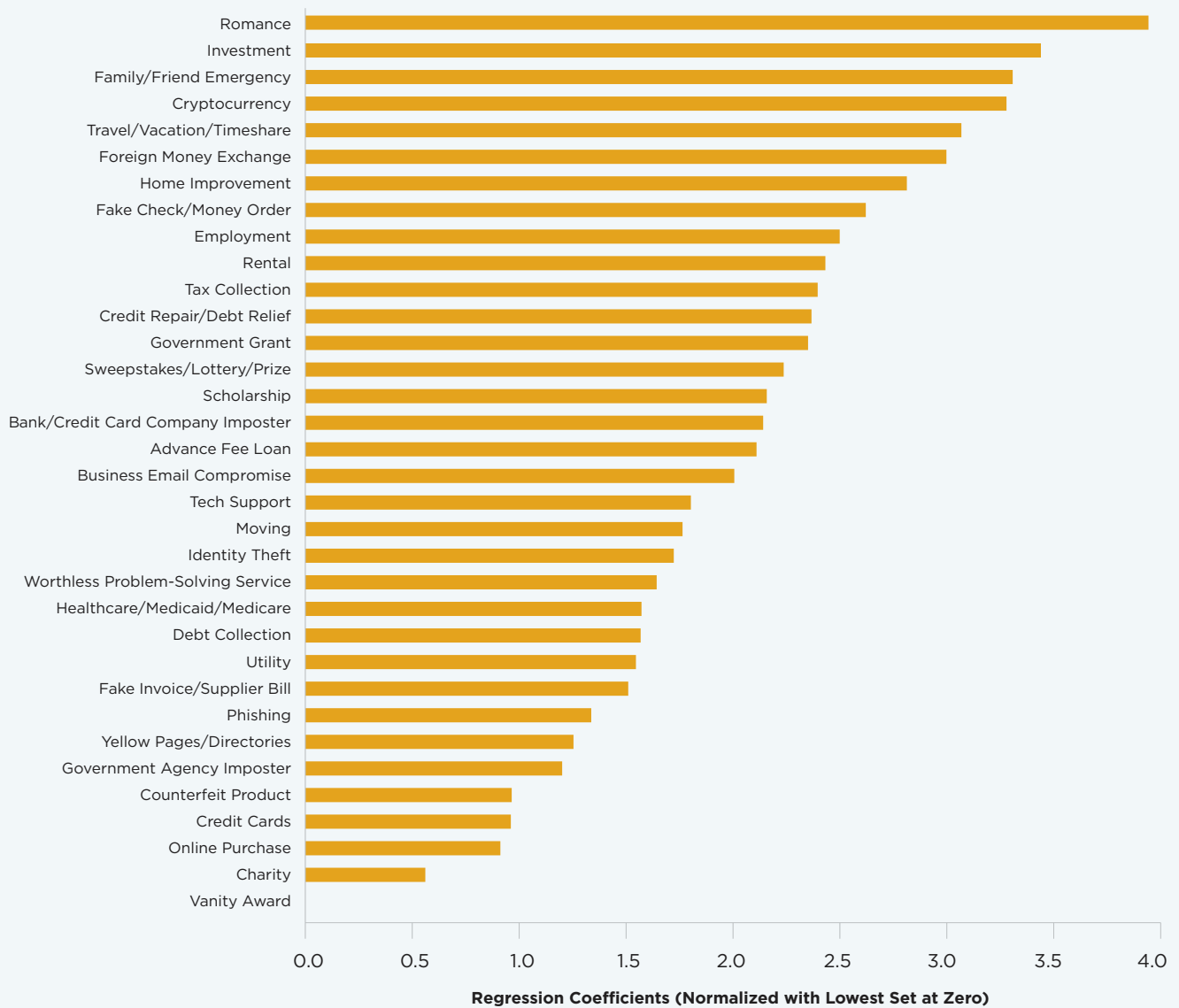
<sup>1</sup> Some of the following scam types were reported by businesses. Visit [BBB.org/ScamTips](https://www.bbb.org/scam-tips) for scam type definitions.

### Once victimized, what types of scams lead to more money lost?

As reported in Figure 3, victims of romance scams lose the most amount of money relative to other types of scams. Investment and cryptocurrency scams as well as false claims of a family/friend emergency are the next most likely scam types to result in a monetary loss.

FIGURE 3

#### *Scam Type and Monetary Amounts of Victimization*



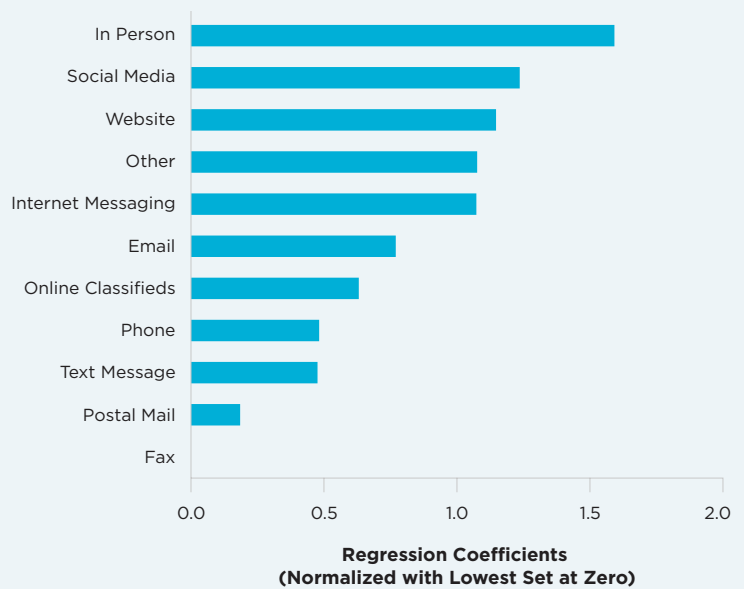
**In-person contact is most likely to lead to victimization, followed equally by social media and website contacts.**

For the scams' means of contact, Figures 4 and 5 display the relative factors of success for incidence and monetary amounts respectively. In-person contact is most likely to lead to victimization, followed equally by social media and website contacts. In-person contacts are most often scams related to home improvement and counterfeit products, whereas social media and website contacts are most frequently online purchase scams as well as scams involving counterfeit products.

In terms of amounts lost when victimized, in-person and text message contacts are the most successful. Even though scams perpetrated via fax also seem to inflict large monetary losses, there is little indication they lead to any victimization at all.

**FIGURE 4**

*Means of Contact and Incidence of Victimization*



**FIGURE 5**

*Means of Contact and Monetary Amounts of Victimization*

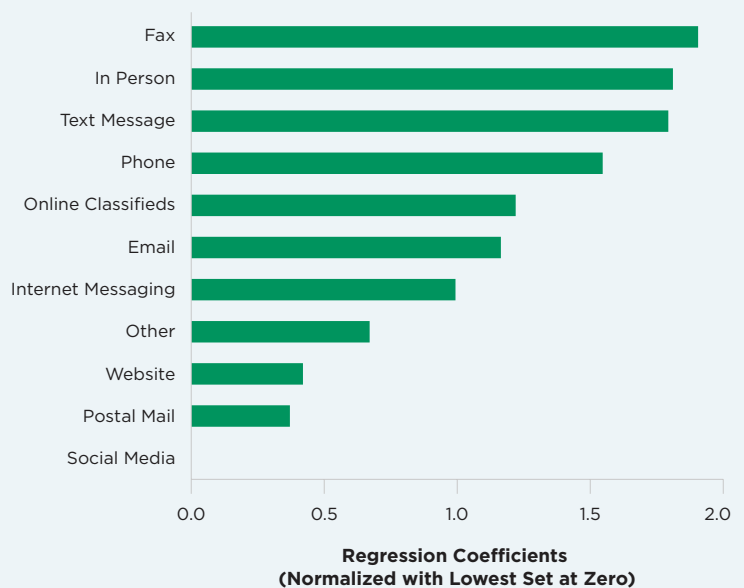




TABLE 1

*Reporting and Victimization by Gender*

GENDER	REPORTING	VICTIMIZATION	MEDIAN LOSS
<b>Female</b>	65%	67%	\$112
<b>Male</b>	35%	33%	\$205
<b>Overall</b>	100%	100%	\$150

TABLE 2

*Reporting and Victimization by Age*

AGE	REPORTING	VICTIMIZATION	MEDIAN LOSS
<b>18-24</b>	7%	10%	\$113
<b>25-34</b>	18%	21%	\$112
<b>35-44</b>	19%	22%	\$124
<b>45-54</b>	19%	19%	\$136
<b>55-64</b>	18%	16%	\$180
<b>65+</b>	18%	12%	\$300
<b>Overall</b>	100%	100%	\$150

Women are much more likely than men to report an attempted scam (65% to 35%). They are also twice as likely as men to report being victimized (67% to 33%). But conditional on being victimized, men lose more money than women (\$205 to \$112, median losses). See Table 1. Reported victimization tends to decrease in age, though once victimized amount lost increases. See Table 2.

In order to understand how reported victimization is affected by income, education, and other demographic variables, we combined BBB Scam Tracker data with zip code variables from the U.S. Census.<sup>2</sup> Specifically, we matched demographic averages at the zip code level with the victim's reported zip code. In a two-stage regression, we estimated how these factors affected both victimization and dollars lost.

<sup>2</sup> Reports from Canada are excluded from this analysis.

This regression controls for all collected scam variables (e.g., scam type, means of contact) and other reported variables (e.g., age, gender, and student status). The results shown in Table 3 (“victimization” and “dollars lost” columns) indicate that those reporting from zip codes with a larger portion of Black, Hispanic, Asian, and other racial minorities or a population less likely to have GED or high school equivalent education are more likely to be victims of a scam. However, none of these factors is associated with losing more money, conditional on being a victim. Those reporting from zip codes with a higher than average median income are more likely to be victimized and lose more money.

When interpreting these results, it is important to address any potential reporting bias in the BBB Scam Tracker data. Specifically, one cannot be certain that victims not reporting to BBB Scam Tracker are generally similar to those who do. To identify the impact of such a potential bias, we regressed the per capita number of BBB Scam Tracker reports per zip code on demographic averages discussed above. The regression results shown in Table 3 (“reporting” column) indicate more reported incidents of scams in zip codes with less diverse populations and people who are more likely to have at least a high school education. In other words, if there is a reporting bias, it means reports will more often occur in regions with populations which are less diverse and more likely to have a degree. Therefore, the findings above regarding victimization rates among Black, Hispanic, Asian, and other racial minorities and those with less likely to have GED or high school equivalent education stand firm despite potential under reporting from these populations.

Those reporting from zip codes with a larger portion of minorities or a population less likely to have GED or high school equivalent education are more likely to be victims of a scam.

**TABLE 3**  
*Regression Coefficients with Zip Code Level Characteristics in U.S.*

ZIP CODE LEVEL CHARACTERISTICS	REPORTING		VICTIMIZATION		DOLLARS LOST	
	COEFFICIENT	STD. ERR	COEFFICIENT	STD. ERR	COEFFICIENT	STD. ERR
<b>Renter Occupied %</b>	-1.9E-03***	1.2E-04	0.106**	0.052	0.268***	0.082
<b>Median HH Income</b>	-1.55E-09	1.02E-09	1.4E-03***	4.6E-05	4.E-03***	7.4E-04
<b>Minority %</b>	-1.1E-04**	5.45E-05	0.182***	0.030	0.089*	0.048
<b>PT Work %</b>	-3.2E-04	1.2E-04	-0.556***	0.125	-0.495**	0.202
<b>&gt; GED %</b>	2.3E-04**	9.86E-05	-0.290***	0.058	-0.013	0.093
<b>Constant</b>	2.0E-03	1.4E-04	0.766***	0.099	4.792***	0.140

STATISTICAL SIGNIFICANCE: \*\*\*1%, \*\*5%, \*10%

Finally, a geo-demographic view of victimization can be constructed by examining some of the most affected zip codes. Table 4 provides the 20 zip codes with highest per-capita rates of victimization. This perspective shows that victimization spans the geographic United States, from Aleutian Islands of Alaska to southern Florida. Many of the most affected zip codes are rural and more likely to have less diverse populations and zip codes with residents who are less likely to have a high school education or GED equivalent (e.g., Adamsville, OH; Bettsville, OH; Deepwater, NJ; Land O' Lakes, WI; New Freeport, PA; North Stratford, NH; and Richeyville, PA).

Exceptions to this pattern are found in urban areas with a considerably high proportion of at least a high school education (e.g., Miami Beach, FL and San Jose, CA). Other highly affected zip codes have a significant minority (Black, Hispanic, Asian, and other racial minorities) population who are less likely to have a high school education or GED equivalent. For instance, the most affected zip code is Adak, AK, which has a sizable portion of Native Americans. Other highly affected zip codes have a more diverse population with more representation of Black residents and zip codes with residents who are less likely to have a high school education or GED equivalent (Little Rock, AR; Mobile, AL; and Muskegon, MI).

**TABLE 4**

*Top 20 Most Affected Zip Codes in U.S. (Percentiles based on sampled zip codes)*

	ZIP CODE	CITY	STATE	MINORITY		>GED		MEDIAN INCOME	
				%	%-ILE	%	%-ILE	\$	%-ILE
01	99546	Adak	AK	80.0	97.1	18.0	9.2	88,750	89.5
02	08023	Deepwater	NJ	5.8	20.4	16.0	5.7	48,958	42.4
03	33109	Miami Beach	FL	6.7	23.6	67.0	93.7	166,976	99.7
04	44815	Bettsville	OH	3.0	6.9	13.0	2.5	37,813	17.0
05	63039	Gray Summit	MO	4.1	13.3	26.0	29.7	44,521	32.2
06	02802	Albion	RI	3.8	11.8	30.0	40.9	48,456	41.2
07	14480	Lakeville	NY	7.3	25.6	24.0	24.0	45,865	35.5
08	77629	Nome	TX	24.2	64.3	32.0	45.9	52,813	50.6
09	95113	San Jose	CA	56.9	90.9	64.0	91.9	34,345	10.9
10	04455	Lee	ME	10.1	34.1	33.9	50.5	54,167	53.1
11	15358	Richeyville	PA	3.5	10.0	30.2	41.9	41,429	24.5
12	54540	Land O' Lakes	WI	3.2	8.3	38.8	61.0	33,203	9.3
13	49440	Muskegon	MI	33.6	75.4	32.0	45.9	21,397	0.8
14	15352	New Freeport	PA	2.2	2.6	11.9	1.7	35,125	12.1
15	72201	Little Rock	AR	30.6	72.3	53.0	82.1	48,947	42.3
16	03590	North Stratford	NH	3.4	9.5	18.0	9.2	28,393	4.1
17	36602	Mobile	AL	44.3	84.0	38.5	54.7	20,227	0.5
18	43802	Adamsville	OH	2.0	1.8	20.0	13.6	42,500	27.0
19	05455	Fairfield	VT	3.1	7.5	30.0	40.9	66,071	71.0
20	04539	Bristol	ME	1.3	0.3	39.0	61.2	56,786	57.7



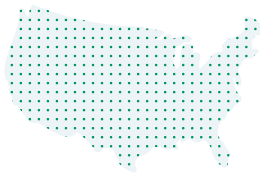
# Impact of COVID-19

**The analysis over the COVID-19 period (starting on March 15, 2020) reflects similar patterns of reported scams and victimization. However, there are a few differences worthy of attention.**

## REPORTED SCAMS

There are notable increases in reporting of scams during the COVID-19 period, particularly for online purchase, COVID-19-related, and phishing scams. COVID-19-related scams peaked during the start of the pandemic, followed by a peak in online purchase scams. Reports of phishing scams pick up later in the summer of 2020. See again Figure 1. It is reasonable to suspect that the uptick in reported scams to BBB Scam Tracker owes in part to the fact that people spent more time online during the pandemic. However, the observation that the trend did not occur consistently across all scam types suggests there were, in fact, more attempted scams during the COVID-19 period.

The rise and fall of COVID-19 scams coincide with the period of intense shortages from March to June 2020.



**MOST COMMON COVID-19 SCAM**  
**United States**



**RELATED TO MASKS AND OTHER PERSONAL PROTECTIVE EQUIPMENT (PPE)**





**MOST COMMON COVID-19 SCAM**  
**Canada**



**PET-RELATED SCAMS**

This includes both scams related to the purchasing of pets due to increased social isolation from COVID-19, as well as scammers using COVID-19 as an excuse or method to carry out the scam (e.g., claiming there are increased shipping costs or delays).

## COVID-19 SCAM HIGHLIGHTS IN 2020<sup>3</sup>

	 UNITED STATES	 CANADA
HIGHLIGHTS	<b>6.9%</b> of total reports	<b>6.1%</b> of total reports
	<b>66%</b> Reported losing money	<b>53%</b> Reported losing money
	<b>\$86</b> Median amount lost (USD)	<b>\$206</b> Median amount lost (CAD)
TOP MEANS OF CONTACT FOR THOSE WHO LOST MONEY	<b>38%</b> Website	<b>32%</b> Website
	<b>25%</b> Social media	<b>28%</b> Social media
	<b>17%</b> Email	<b>20%</b> Email
MOST COMMON TYPES OF SCAMS	<b>26%</b> Masks	<b>20%</b> Pets
	<b>13%</b> Pets	<b>12%</b> Employment
	<b>12%</b> Employment	<b>11%</b> Masks
TOP ISSUES	<b>27%</b> Shipping	<b>22%</b> Refund
	<b>18%</b> Refund	<b>17%</b> Shipping
	<b>8%</b> Counterfeit product	<b>10%</b> Counterfeit product

## Looking forward

- 01** Mask scams have declined significantly from its high in April/May.
- 02** Pet scams and employment scams are on the rise.
- 03** Vaccine scams were only about 0.8% of total in 2020.

<sup>3</sup> From January through December 2020

## REPORTED VICTIMIZATION

### Victimization Rates

We find no evidence that the rates of victimization across non-COVID-19-related scams changed substantially during the COVID-19 period.

### Monetary Losses

There is, however, an increase in reported monetary losses during the COVID-19 period, particularly in online purchases and phishing scams. See last row in Table 5.

### Victimization by Gender

Consistent with general trends, women reported more often being victimized than men during the COVID-19 period and men reported more monetary losses. By contrast, COVID-19's impact appears less systematic across age. This is evident in Table 5 for the most prevalent scams during the COVID-19 period.

### Geodemographic Rates

The geodemographic pattern of victimization during the COVID-19 period is consistent with the general trends. Specifically, those reporting from zip codes with residents who are less likely to have a high school education or GED equivalent or a larger portion of minorities are more likely to be victims of a scam during the COVID-19 period. The most severely affected zip codes during the COVID-19 period look very similar to those generally: rural and more likely to have less diverse populations and zip codes with residents who are less likely to have a high school education or GED equivalent or zip codes with a large share of minorities who are less likely to have a high school education or GED equivalent and lower than average median income.

**TABLE 5**  
*COVID-19 Impact on Median Loss Per Victimization*

GENDER/AGE	ONLINE PURCHASES		PHISHING	
	PRE-COVID-19	COVID-19	PRE-COVID-19	COVID-19
<b>Female</b>	\$74	\$90	\$300	\$305
<b>Male</b>	\$99	\$100	\$275	\$400
<b>18-24</b>	\$57	\$107	\$200	\$224
<b>25-34</b>	\$65	\$85	\$237	\$200
<b>35-44</b>	\$77	\$99	\$350	\$490
<b>45-54</b>	\$88	\$98	\$260	\$130
<b>55-64</b>	\$99	\$92	\$300	\$510
<b>65+</b>	\$128	\$90	\$320	\$228
<b>Overall</b>	\$80	\$96	\$295	\$350



# Summary

**More scams were reported during the COVID-19 period relative to prior years, owing mostly to online purchase, phishing, and COVID-19-related scams. Overall, however, there was little change in the rate of victimization during the COVID-19 period relative to prior years.**

## 01

While there is evidence of additional monetary losses during the COVID-19 period, it occurs mostly with online purchase and phishing scams.

## 02

The spell of COVID-19-related scams in spring 2020 involved typically undelivered PPE and sanitation products.

## 03

Women reported victimization more often than men, but in most instances lost less than men in these scams.

## 04

Age does not appear to affect the rate of victimization, though older victims tended to pay more once victimized.

## 05

Consistent with prior years, residents in zip codes with a higher percentage of minorities (Black, Hispanic, Asian, and other racial minorities) and zip codes with a population who is less likely to have a high school education or GED equivalent were more likely to be victimized by scams during the COVID-19 period.



## Methodology

The relative impact of Scam Types and Means of Contact are estimated by a hurdle model regression, which was used because of the high portion of BBB Scam Tracker reports with zero dollars lost.

Not accounting for this aspect of the data may misattribute the impact of factors affecting victimization. The hurdle model simultaneously estimates two stages, the first of which assess the factors of victimization (losses greater than 0) and the second of which assesses the factors affecting monetary losses conditional on victimization (Figures 2-5). Measures of distributional centrality for monetary losses are presented as medians to reduce the effect of unreasonably large-reported victimization amounts (Tables 1, 2, and 5).

# Prevention Tips for Avoiding Scams

The following tips can help you avoid scams. Prior knowledge about scammer tactics has been shown to help consumers avoid losing money to scams.<sup>4</sup>



## 01

**If the deal looks too good to be true, it probably is.**

Scammers offer hard-to-match prices for sought-after products. Proceed with caution with these types of offers.

## 02

**Before you buy, do your research.**

If you are purchasing from a new website or business, take your time and conduct additional due diligence before you make that purchase.

## 03

**Be careful purchasing sought-after products.**

Scammers took advantage of the COVID-19 pandemic by offering hard-to-find products at attractive prices.



## 04

**Use secure and traceable transactions and payment methods.**

Avoid paying by wire transfer, prepaid money card, gift card, or other non-traditional payment methods.

<sup>4</sup> *Exposed to Scams: What Separates Victims from Non-Victims?* BBB.org/ExposedtoScams



05

**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. If a business displays a BBB Accreditation Seal, you can verify its legitimacy at [BBB.org](https://www.bbb.org).



06

**Beware of making quick purchases while scrolling social media.**

Did you see an ad for those red shoes you've been searching for, and they're a steal? Like marketers for real companies, scammers have access to the tools they need to learn about your buying behaviors, offering up exactly what you want at enticing prices.



07

**Avoid clicking on links or opening attachments in unsolicited emails.**

Links, if clicked, can download malware onto your computer, smart phone, tablet or whatever electronic device you're using at the time, allowing cyberthieves to steal your identity. Be cautious even with email that looks familiar; it could be fake. If it looks unfamiliar, delete it and block the sender.



08

**Never share personally identifiable information with someone who has contacted you unsolicited, whether it's over the phone, by email, on social media, even at your front door.**

This includes banking and credit card information, your birthdate, and Social Security/Social Insurance numbers.



09

**Use extreme caution when dealing with anyone you've met online.**

Scammers use dating websites, Craigslist, social media, and many other sites to reach potential targets. They can quickly feel like a friend or even a romantic partner, but that is part of the con for you to trust them.



## AUTHORS

### Linli Xu

#### UNIVERSITY OF MINNESOTA

*Assistant Professor of Marketing at the Carlson School of Management, University of Minnesota*

Professor Xu teaches courses on Marketing Analytics. She has a PhD in Marketing from the University of Southern California. Her research focuses on advertising, media, and marketing in the automotive industry and has appeared in journals such as the *Journal of Marketing, Management Science*, and *Marketing Science*.

### Yi Zhu

#### UNIVERSITY OF MINNESOTA

*Associate Professor of Marketing at the Carlson School of Management, University of Minnesota*

Professor Zhu teaches courses on Marketing Strategy and Marketing Analytics. He has a PhD in Marketing from the University of Southern California. His research focuses on online auctions, consumer search, advertising, media slant, sharing economy, and Chinese economy. It has appeared in journals such as the *Journal of Marketing Research, Management Science*, and *Marketing Science*.

### Anthony Dukes

#### UNIVERSITY OF SOUTHERN CALIFORNIA

*Professor of Marketing at the Marshall School of Business, University of Southern California*

Professor Dukes is department chair. He has a PhD in Economics from the University of Pittsburgh. His research focuses on e-commerce, retailing, and distribution channels and has appeared in journals such as the *Journal of Marketing Research, Management Science*, and *Marketing Science*.

## CONTRIBUTORS

We pay special thanks to key individuals with the BBB Institute for Marketplace Trust, the International Association of Better Business Bureaus, and the BBB Serving Minnesota & North Dakota who helped make this report possible.

#### **Dr. Rubens Pessanha, MBA, PMP, GPHR, SPHR, SHRM-SCP**

*IABBB Senior Director of Research & Development*

#### **Dr. Sean Xiangwen Lai**

*IABBB Research & Development Specialist*

#### **Matt Scandale**

*IABBB Senior Data Analyst*

#### **Susan Adams Loyd**

*CEO of BBB Serving Minnesota & North Dakota*

#### **Lisa Jemtrud**

*Vice President of Community Relations of BBB Serving Minnesota & North Dakota*

#### **Melissa Trumpower**

*BBB Institute Executive Director*

#### **Melissa Bittner**

*BBB Institute Curriculum Development and Training Manager*

## BBB RESOURCES

# Other Research by the BBB Institute

**As a non-partisan, neutral organization, BBB Institute is able to produce research that provides fresh insights into the scam landscape. A few examples of our research include:**

### **Annual BBB Scam Tracker Research Report**

Released each year during Consumer Protection Week, this report provides fresh insights from the previous year using data from BBB Scam Tracker data. The Risk Report was the first research report to introduce the BBB Risk Index, a new three-dimensional measure of scam risk based on exposure, susceptibility and monetary loss.

### **Research on Specific Scam Types**

BBB Institute publishes reports about the impact of specific scam types. Following the COVID-19 pandemic, we released reports about employment and online purchase scams.

### **Research on Specific Demographic Groups**

BBB Institute publishes research about the impact of scams on specific cohorts. In 2019, we published the *Military Consumers & Marketplace Trust: An Analysis of Marketplace Challenges Facing the Military Community*.

### **Scams and Small Businesses**

In our 2018 research project with the Council of Better Business Bureaus, *Scams and Your Small Business*, we used survey data and BBB Scam Tracker data to provide insights on scams targeting small businesses.

**[A full list of BBB Institute research can be found online.](#)**

## How to Collaborate with BBB on Research

As stated earlier, consistent research about challenges facing a trustworthy marketplace are critical to protecting consumers and leveling the playing field for legitimate businesses. BBB Institute seeks the opportunity to collaborate with organizations and universities interested in publishing new insights that empower us to foster a fair and trustworthy marketplace for all consumers and ethical businesses.

**If you are interested in exploring how you could work with us, please contact BBB Institute at [Institute@IABBB.org](mailto:Institute@IABBB.org).**



## About BBB Institute

The BBB Institute for Marketplace Trust (BBB Institute) is 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 trustworthy 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, and publishing research that provides critical insights for consumers and business owners.

Learn more at [BBBMarketplaceTrust.org](https://BBBMarketplaceTrust.org).