INSTITUTE for MARKETPLACE TRUST℠

BBB

2024

BBB Scam Tracker℠

Risk Report

INSTITUTE for MARKETPLACE TRUST℠

2024 BBB Scam Tracker℠ Risk Report

TABLE OF CONTENTS

Introduction

The BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the International Association of Better Business Bureaus, is pleased to present the *2024 BBB Scam Tracker Risk Report*. This annual report analyzes data that individuals and businesses submitted to BBB Scam Tracker℠ (BBB.org/ScamTracker) in 2024. The findings shed light on how scams are perpetrated, who is being targeted, which scams have the greatest impact, and which behaviors and factors may affect a person's susceptibility. Highlights of the 2024 report are provided in Figure 3.

Scams hurt both consumers and businesses by undermining trust in the marketplace. A trustworthy marketplace requires an empowered and knowledgeable public, and ethical businesses that are proactively working to stop scammers and protect their customers.

BBB Institute collaborates with like-minded partners to expand our programs and consumer education activities, evaluate which efforts are working, and continually update them on the basis of internal and external research and data. The findings in this report will allow us to create timely consumer education resources aimed at empowering people to protect themselves and their families. These resources will be distributed via the expansive network of BBBs that serve communities throughout the United States and Canada.

About BBB Scam Tracker

The *BBB Scam Tracker Risk Report* uses data from BBB Scam Tracker, an online platform where people and businesses can report scams. The BBB® reviews and posts these reports, allowing the public to search and determine if they are being targeted.

According to a survey of people who filed BBB Scam Tracker reports in 2024,[1] 44.7% of visitors said they visited the BBB Scam Tracker website to find out if they were experiencing what could be a scam, and 30.6% of those said BBB Scam Tracker helped them avoid losing money when targeted by a scam. With more than 2.4 million people visiting the platform in 2024,[2] we estimate BBB Scam Tracker helped people avoid losing more than $43 million in 2024 alone (Figure 1). We extend our thanks to the hundreds of thousands of people who chose to speak out and warn others by reporting scams to BBB Scam Tracker.

FIGURE 1 **2024 BBB Scam Tracker impact**

2,421,160

Unique visitors to BBB Scam Tracker

44.7%

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

30.6%

Said BBB Scam Tracker helped them avoid losing money

$130

Median U.S. dollar amount saved

$43,052,244

Estimated dollar amount people avoided losing thanks to BBB Scam Tracker

[1] Web-intercept survey with 2,650 unique respondents who visited BBB Scam Tracker in January 2024. Respondents could choose multiple reasons for visiting BBB Scam Tracker.

[2] Adobe Analytics.

Snapshot of 2024

The data from BBB Scam Tracker reports help us understand how scams are being perpetrated in the marketplace. In 2024, BBB Scam Tracker published more than 81,000 reported scams. We classified scam reports submitted by individuals and businesses across the United States and Canada into 33 scam types and an "other" category that represented 6.9% of all reports. See Appendix A for a full glossary of scam types.

Data collected from each scam report includes a description of the scam, the dollar value of any loss, and information about the contact and payment methods. Demographic data (age, gender, military status, and postal code) about the person targeted by the scam is optional for businesses and individuals. See Appendix B and Appendix C for detailed data by scam type.

Reported median dollar increases

In 2024, susceptibility (the percentage of people who reported losing money when exposed to a scam) decreased from 52.0% in 2023 to 44.4% in 2024 (Figure 2). Reported median dollar loss increased from $100 in 2023 to $130 in 2024.

Changes to list of riskiest scam types

Although the top two riskiest scams remained the same as those reported in 2023, there were some changes further down the list this year. For the first time since we began publishing the report in 2016, online purchase scams did not rank among the top three riskiest scams. Romance/friendship scams rose to No. 3 riskiest. More details about the list can be found on page 14.

How scammers engaged their targets

In 2024, the top three contact methods resulting in a reported monetary loss remained the same as in 2023: social media, website, and email. Credit cards remained the top reported payment method, followed by bank account debit and online payment system (digital payment app). Reports with a loss via cryptocurrency rose from 3.0% in 2023 to 4.8% in 2024. You can find more information on pages 26–32.

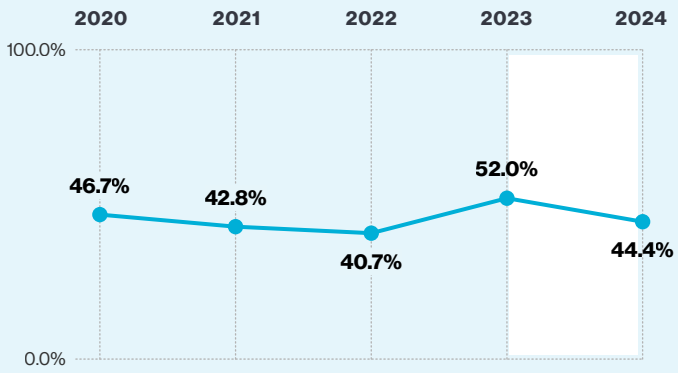
FIGURE 2

Snapshot of risk (2020–2024)

SUSCEPTIBILITY

Percentage of reports that include a dollar loss

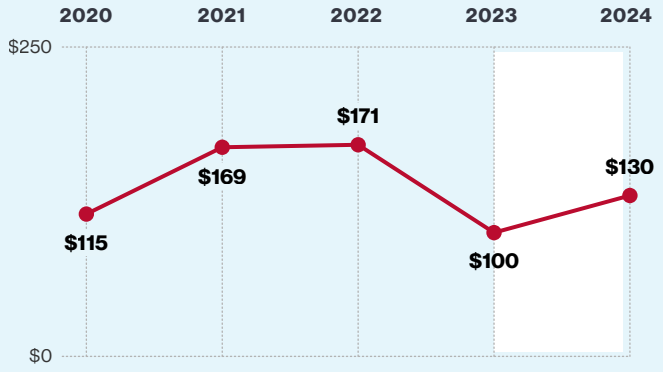
14.6%
DECREASE from 2023



MONETARY LOSS*

Median reported dollar loss

30.0%
INCREASE from 2023



* *Median dollar loss was calculated only for scams with a reported loss.*

FIGURE 3

2024 BBB Scam Tracker Risk Report HIGHLIGHTS

OVERALL SUSCEPTIBILITY

LIKELIHOOD OF LOSS **44.4%**

14.6% **DECREASE** from 2023

OVERALL MONETARY LOSS

MEDIAN $ LOSS[3] **$130**

30.0% **INCREASE** from 2023

TOP 3 RISKIEST SCAMS REPORTED BY CONSUMERS[4]

1 Investment/cryptocurrency scams

Investment/cryptocurrency scams are the No. 1 riskiest scam type again this year, with a reported median dollar loss of $5,000 and 80.1% of reports with a monetary loss. According to survey respondents, 26.2% of those who reported investment/cryptocurrency scams said the **scammer spent time building a romance or a friendship before perpetrating the scam.**

2 Employment scams

Employment scams remained the No. 2 riskiest scam type, with a median dollar loss of $1,500; **it made up more than 14% of all reported scams.**

3 Romance/ friendship scams

Romance/friendship scams rose to No. 3 riskiest for the first time since we began publishing this report. This scam had the **highest median dollar loss ($6,099) of all scam types.**

MOST REPORTED SCAM TYPE

Online purchase scams dropped from the top three riskiest for the first time since 2016. This scam type **made up more than 30% of all scams reported to BBB Scam Tracker, with 87.5% reporting a dollar loss.**

AGE GROUPS MOST AFFECTED

People ages 65+ reported the **highest median dollar loss ($160)** of all age groups **followed by people ages 18–24 ($150).** People ages 35–54 submitted a higher percentage of reports with a loss than other age groups.

CONTACT METHODS

Email was the most reported contact method in 2024, but **social media** was the top reported payment method with a monetary loss.

MOST IMPERSONATED

Publishers Clearing House was the organization most often impersonated by scammers in 2024, according to reports submitted to BBB Scam Tracker. The U.S. Postal Service dropped from No. 1 to No. 2 on the list.

[3] Median dollar loss was calculated only for scams with a reported loss.

[4] The list of riskiest scams is determined through a unique formula, the BBB Risk Index. Learn more on page 9.

FIGURE 3

2024 BBB Scam Tracker Risk Report HIGHLIGHTS

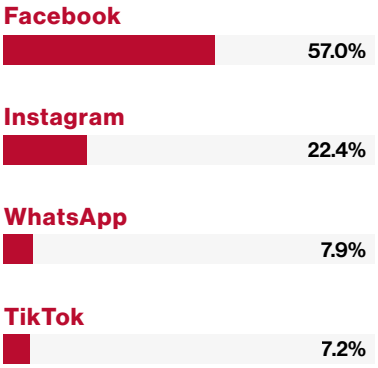
SURVEY RESEARCH[5] HIGHLIGHTS

29.6%
reported that their **mental health was impacted by the scam incident.** About 53% of respondents reported feeling **anxiety, stress, and/or trauma** after the engagement.

36.2%
reported that the scam incident **involved social media.**

Almost 50% of respondents said the engagement **began when they responded to a social media ad/post.**

The **top platforms** on which survey respondents reported engaging with scammers were:



Of those who reported an **investment scam,**

45.3%
said the incident involved **cryptocurrency**;

23.8%
said the scam was **perpetrated by an online contact.**

40.1%
of those who reported employment scams said **flexibility to work from home was the top motivating factor** for engaging with the scammer.

[5] A survey was distributed to those who submitted a scam to BBB Scam Tracker in 2024; 3,300 respondents completed the survey.

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

To better understand which scam types pose the highest risk, we assess scams on the basis of three factors: exposure,[6] susceptibility, and monetary loss. This unique formula makes up 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 submitted and enables BBB Institute and its partners to better target scam-prevention outreach efforts.

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 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 higher amounts of money.

The BBB Risk Index does not factor in the non-financial impacts of scams. According to our survey research, people also reported losing time (66.3%) and personal information (38.9%) (Figure 5).[7]

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)
× 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 included 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.

[6] Exposure is limited by the nature of self-reporting; the percentage of those who reported to BBB Scam Tracker does not necessarily match the percentage of people in the full population who were targeted by scams.

[7] A survey was distributed to those who submitted a scam to BBB Scam Tracker in 2024; 3,300 respondents completed the survey.

We also asked people about the emotional impact of being targeted by a scam[8] (Figure 6). The No. 1 emotion they reported was anger (60.3%), followed by loss of trust (54.0%) and anxiety/stress/trauma (53.5%).

A breakdown by age group highlights some interesting differences (Figure 7). Anxiety, stress and trauma were the top emotions reported by people between the ages of 25 and 44, while anger was the top emotion reported by all other age groups. Younger people reported higher percentages of feeling shame/embarrassment, strained relationships, and guilt.

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

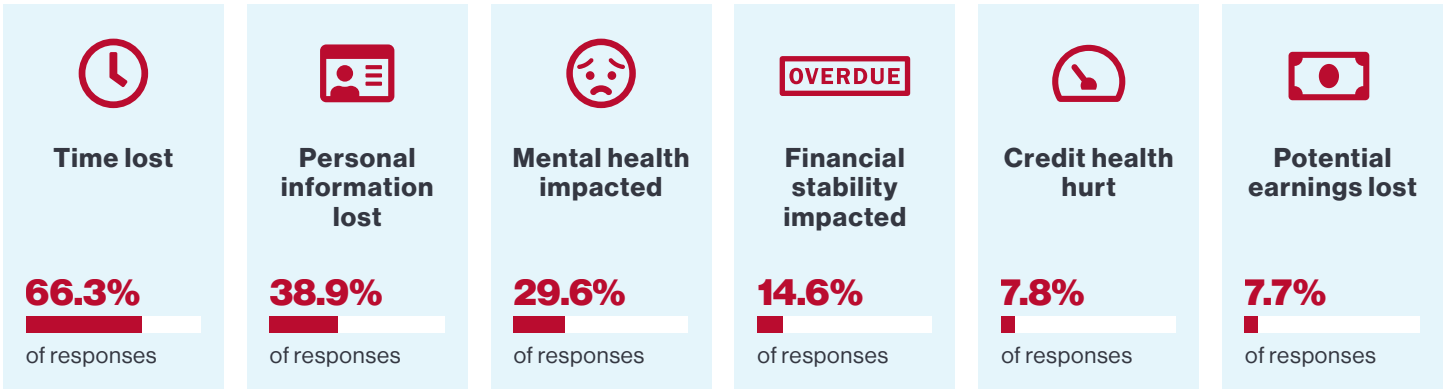
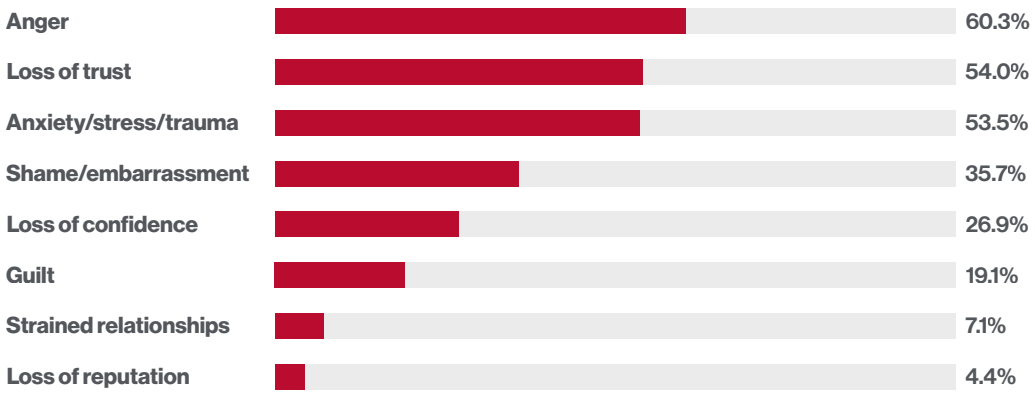


FIGURE 6 **Top emotions/impact of being targeted by a scam**

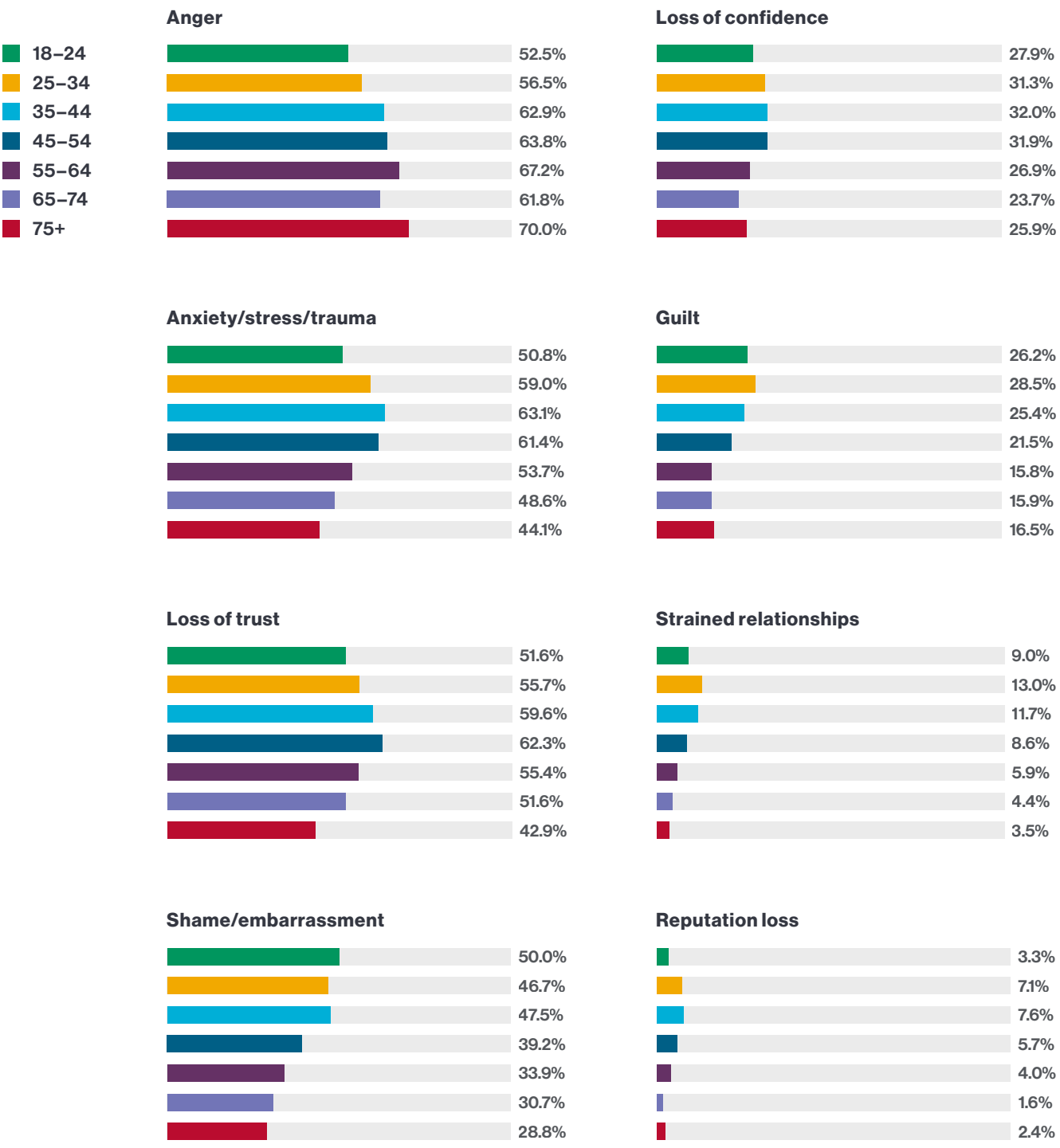


[8] If you or someone you know is struggling with mental health challenges or experiencing feelings of hopelessness or distress, it's important to seek help. Contact a trusted friend, family member, or mental health professional. If you are in immediate danger or need urgent support, please contact emergency services or a suicide prevention hotline in your area.

- In the U.S., you can call or text the **Suicide & Crisis Lifeline at 988** or visit **988lifeline.org** for free, confidential support available 24/7.
- In Canada, you can call **Talk Suicide Canada at 1-833-456-4566 or text 45645**, available 24/7. You can also visit **talksuicide.ca** for resources and support.

FIGURE 7

Emotional impact of being targeted by a scam (by age)



In their own words

We asked survey respondents to describe in their own words how the scam incident made them feel. Included below is a sampling of those responses[9].

I felt awful and betrayed. Leary of ordering anything ever again other than a name brand I am familiar with.

Very insecure. I don't feel like I can trust any financial institution. They did not believe me, and now I am liable for that amount that I cannot pay back. So I am stressed about that and my credit score has gone down after working so hard on it.

Made me not want to answer my phone which is bad because I never know who is calling me with my many health problems and from where. It has been so stressful and wearing my nerves down and I hate that they are targeting me in this way. I just want things to go back to when phone calls were important and beneficial to me.

Sad and depressed[10].

Frustrated. Starting a new business has enough hurdles, but companies trying to take advantage by charging you $ to do things you've already done and threatening fines if not is pretty damn low.

I felt betrayed. I explained to the scammer that I was going through a divorce. I needed that house. He made me feel like the house was going to be mine to only find out, it was a scam and I ended up homeless.

Humiliated, fearful of identity theft during a very vulnerable time. Single mom of two girls, solo income, new small business owner. Thought I would get some relief with this grant and now I'm worried about identity and financial theft with all of the info they have.

[9] These survey responses were edited for grammar, brevity, and clarity.

[10] If you or someone you know is struggling with mental health challenges or experiencing feelings of hopelessness or distress, it's important to seek help. Contact a trusted friend, family member, or mental health professional. If you are in immediate danger or need urgent support, please contact emergency services or a suicide prevention hotline in your area.

- In the U.S., you can call or text the **Suicide & Crisis Lifeline at 988** or visit **988lifeline.org** for free, confidential support available 24/7.
- In Canada, you can call **Talk Suicide Canada at 1-833-456-4566 or text 45645**, available 24/7. You can also visit **talksuicide.ca** for resources and support.

10 riskiest scams reported by consumers in 2024

Each year, BBB Institute publishes its list of the 10 riskiest scam types (Table 1), which we calculate using the BBB Risk Index (Figure 4) and reports submitted to BBB Scam Tracker. In 2024, investment/cryptocurrency scams remained the No. 1 riskiest scam type, with 80.1% of those targeted reporting a monetary loss. The reported median dollar loss ($5,000) was significantly higher than the median dollar loss for scams overall ($130). Employment scams remained the second riskiest scam with a high median dollar loss ($1,500).

Online purchase scams dropped out of the top three riskiest scams on our list despite being the most reported scam type. Meanwhile, romance/friendship scams rose on our list from No. 5 to No. 3 because of their very high median dollar loss ($6,099) and more than 64.5% of targeted people reporting a monetary loss. This significant increase may be due to the rise in financial grooming scams (see page 19).

Romance/friendship scams ranked among the three riskiest scam types for the first time, with the highest reported median dollar loss of all scam types ($6,099).

Scam types with high susceptibility

The scam types with the highest percentage of reports with a dollar loss included online purchase (87.5%), counterfeit product (80.7%), investment/cryptocurrency (80.1%), and moving (74.1%). A full breakout of the scam types with the highest susceptibility can be found on page 53.

Scam types with high median dollar loss

The scam types with the highest median dollar loss included romance/friendship ($6,099), investment/cryptocurrency ($5,000), government grant ($1,825), and home improvement ($1,800). A full breakout of scam types with the highest median dollar loss can be found on page 53.

TABLE 1

10 riskiest consumer scams in 2024

RANK		SCAM TYPE	BBB RISK INDEX	EXPOSURE*		SUSCEPTIBILITY		MEDIAN $ LOSS**	
2024	2023			2024	2023	2024	2023	2024	2023
1	1	Investment/ cryptocurrency	561.6	1.8%	1.7%	80.1%	80.4%	$5,000	$3,800
2	2	Employment	284.3	14.4%	14.8%	17.2%	15.1%	$1,500	$1,995
3	5	Romance/ friendship	196.9	0.7%	0.6%	64.5%	65.7%	$6,099	$3,600
4	3	Online purchase	152.8	30.3%	41.9%	87.5%	82.6%	$75	$71
5	4	Home improvement	138.3	1.4%	1.3%	70.1%	74.7%	$1,800	$2,073
6	7	Phishing/social engineering	56.7	16.4%	12.6%	10.6%	15.0%	$423	$300
7	6	Advance fee loan	39.7	1.7%	1.4%	30.1%	45.3%	$1,000	$900
8	10	Travel/vacation/ timeshare	33.2	2.0%	0.7%	38.0%	59.6%	$573	$543
9	11	Government grant	21.7	0.5%	0.7%	33.3%	33.8%	$1,825	$948
10	9	Tech support	19.2	1.4%	1.9%	31.0%	26.6%	$561	$500

* *Exposure is limited by the nature of self-reporting; the percentage of those who reported to BBB Scam Tracker does not necessarily match the percentage of people in the full population who were targeted by scams.*

** *Median dollar loss was calculated only for scams with a reported loss.*

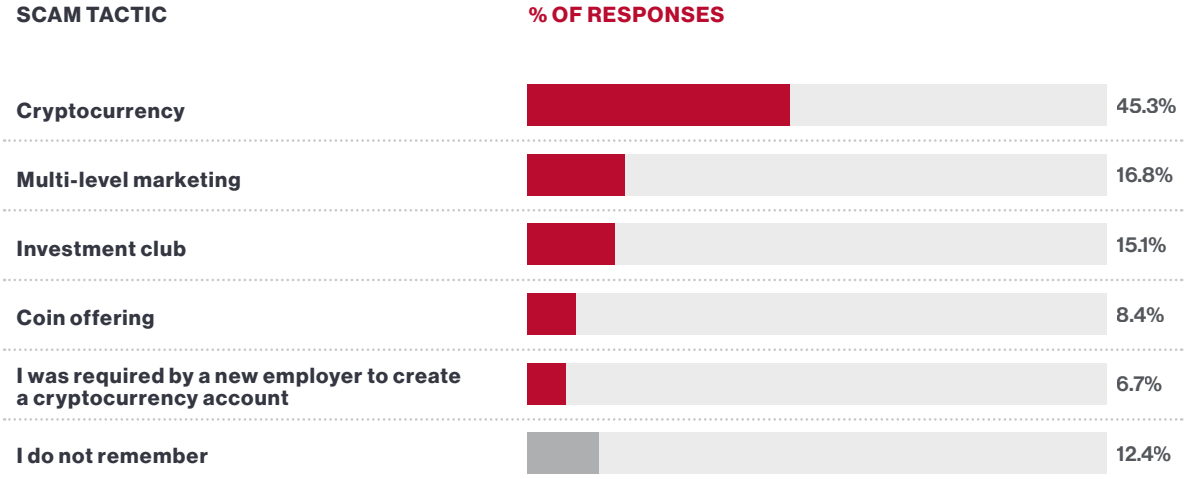
Additional insights on the riskiest scams

To better understand how the three riskiest scams on our list are being perpetrated, we conducted survey research with people who reported scams to BBB Scam Tracker in 2024. Survey respondents said they reported the following scam types: investment and/or cryptocurrency scams (8.6%), employment scams (14.8%), romance/friendship scams (1.6%), business email compromise scams (5.0%), and other scam types (70.0%).

Investment/cryptocurrency scams. Investment scams are perpetrated in a variety of ways, but all promise large returns with little or no risk. About 45% of survey respondents who reported being targeted by an investment scam said the incident involved cryptocurrency (Figure 8).

More than 26% of survey respondents who experienced an investment and/or cryptocurrency scam said the scammer built a relationship with them before perpetrating the scam. Almost 24% said an online contact introduced them to the investment opportunity (Figure 9). Almost 30% reported that they did not research the investment opportunity (Figure 10).

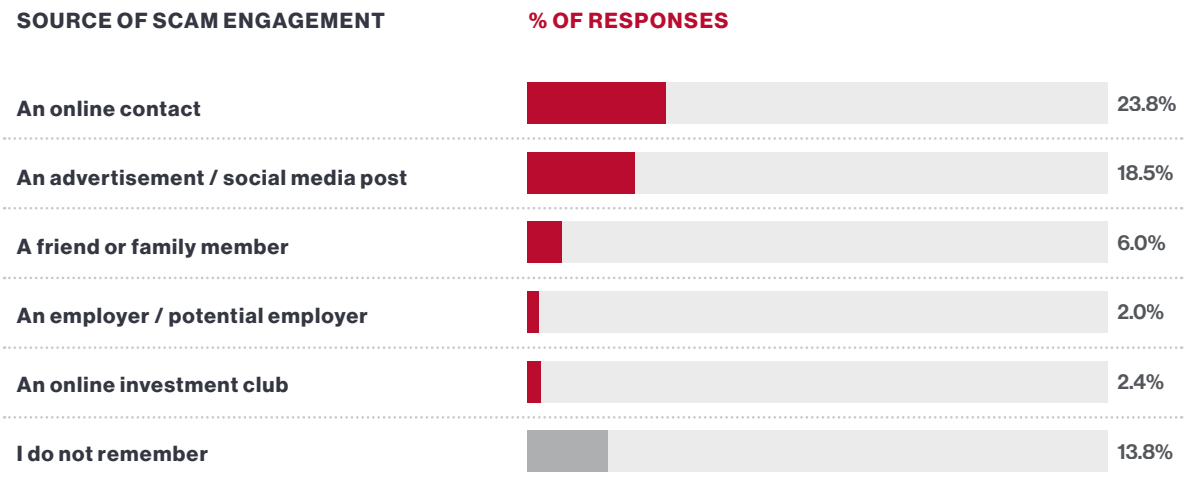
FIGURE 8 **Did the scam involve any of the following scam tactics?**



Responses do not add up to 100% because respondents were asked to select "all that apply."

FIGURE 9

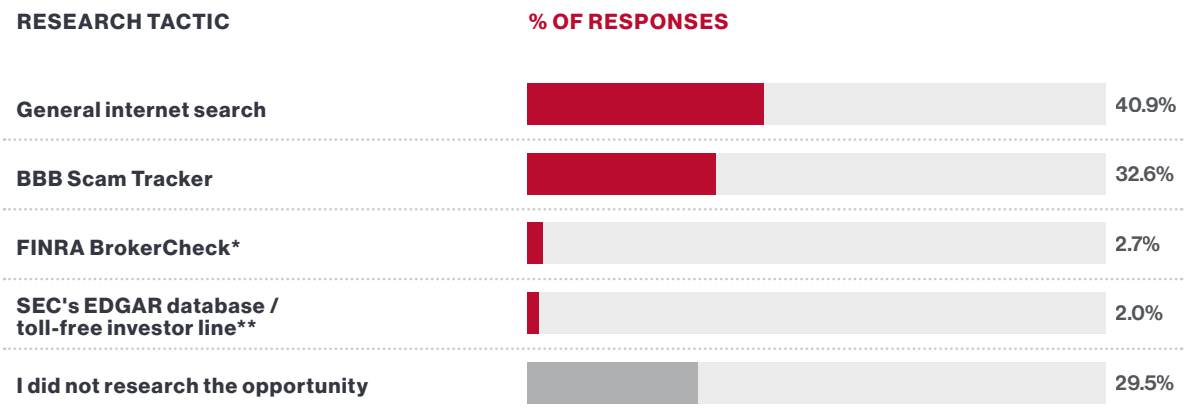
How were you first introduced to this investment opportunity?



Responses do not add up to 100% because the "other" category was not included.

FIGURE 10

If you researched the investment opportunity, which of the following did you do?



Responses do not add up to 100% because respondents were asked to select "all that apply."

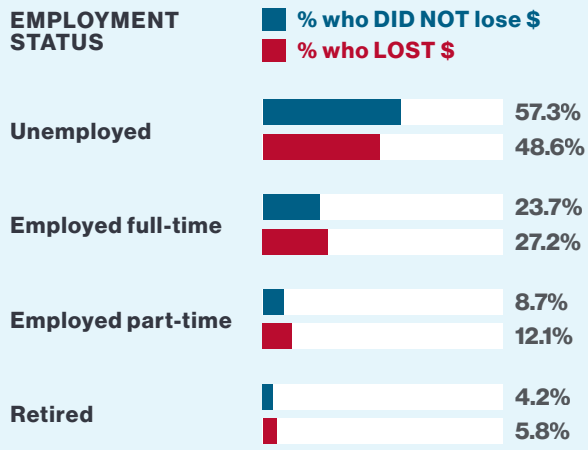
* *BrokerCheck is a free tool from the Financial Industry Regulatory Authority (FINRA) that can help you research the professional backgrounds of investment professionals, brokerage firms and investment adviser firms.*

** *The Security and Exchange Commission's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database provides free public access to corporate information.*

Employment scams. Flexibility to work from home was, by far, the most reported motivational factor for engaging with the scam (Figure 13). Survey respondents who said they were content with their job but were searching for more income were more likely to report losing money than active job seekers (Figure 12).

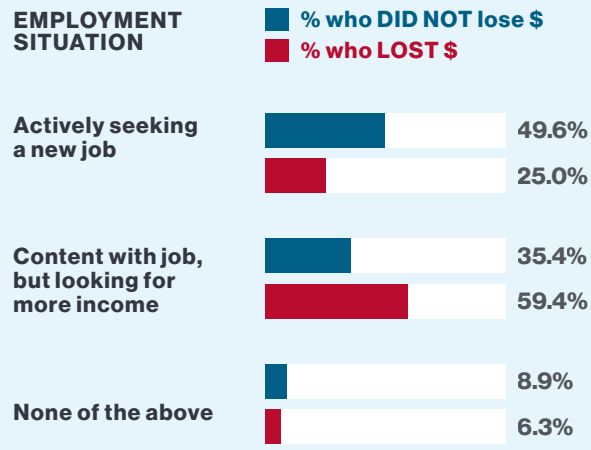
Those who reported being unemployed were more likely to say they did not lose money when targeted by an employment scam. One reason could be that those who are not employed have more time to research offers, while those who are employed may be more distracted and have less time to vet offers from potential employers.

FIGURE 11 **What was your employment status at the time of the scam?**



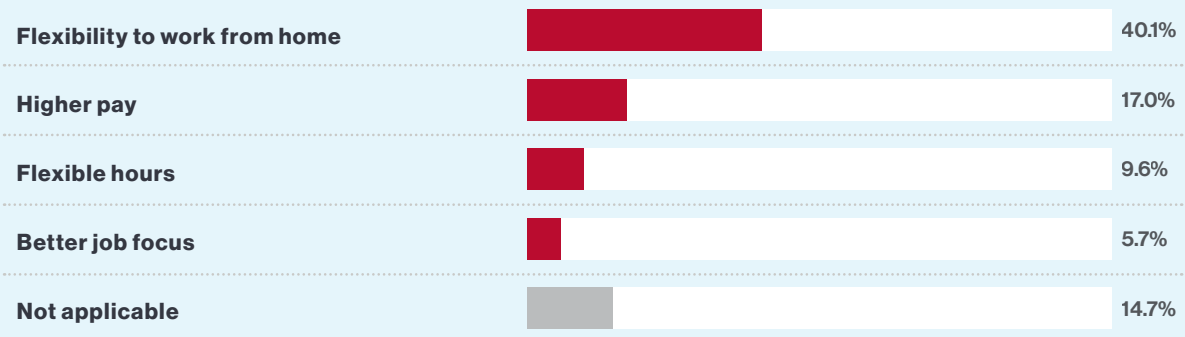
The percentages do not add up to 100% because the "other" category was not included.

FIGURE 12 **If you were employed at the time, which of the following best describes the situation?**



The percentages do not add up to 100% because the "other" category was not included.

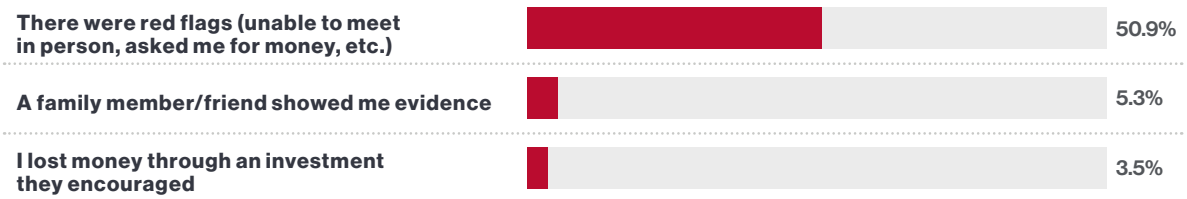
FIGURE 13 **What was the biggest motivational factor that made you engage with the job offer/recruiter?**



The percentages do not add up to 100% because the "other" category was not included.

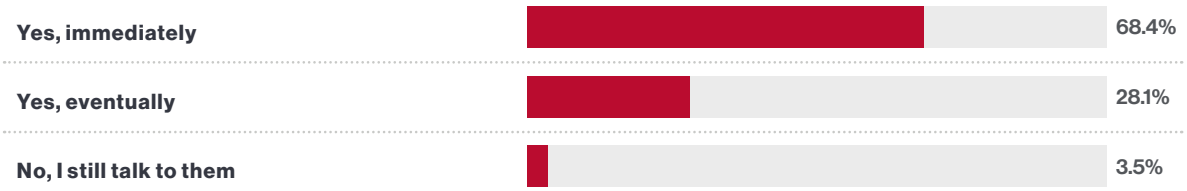
Romance/friendship scams. About 35% of survey respondents reporting a romance/friendship scam said they were encouraged by the scammer to deposit money into a cryptocurrency account. More than 50% said they realized it was a romance/friendship scam because they recognized the red flags such as the person was unable to meet in person or began asking for money (Figure 14). Not all survey respondents ended the engagement immediately once they recognized the scam (Figure 15).

FIGURE 14 **What made you realize the situation was a scam?**



The percentages do not add up to 100% because the "other" category was not included.

FIGURE 15 **Once you realized it was a romance/friendship scam, did you stop engaging with the scammer?**



Financial grooming scams lead to high-dollar losses

In 2024, investment/cryptocurrency scams remained the No. 1 riskiest scam on our list while romance/friendship scams climbed to No. 3 riskiest. Both scam types can be forms of financial grooming, during which the scammer builds a relationship with the potential victim before perpetrating the scam.

Financial grooming scams are often complex and devastating for victims. Scammers with the goal of perpetrating an investment scam take weeks or months to build trust with potential victims. Once trust has been built with the victim, the scammer drops hints about their own financial success. Eventually, the scammer encourages the person to try investing, often in cryptocurrency. It always starts small, with the scammer continuing to build trust over time. The person begins to see their initial investment grow, and the scammer encourages them to invest even more money. But then the person realizes too late, once they've invested a significant amount, that the platform is fake and they can't get their money back.

A newer trend in financial grooming fraud involves employment scams. Scammers hire people and insist on paying them in cryptocurrency. The new hires are told to open a cryptocurrency account, which requires them to deposit money. When it's time to access their pay, they are required to deposit more funds or pay a fee or taxes.

Scammers build trust before urging targets to invest in cryptocurrency.

The following scam report was submitted in Florida.[11]

I met the scammer on TikTok, and we talked for a week. He said he worked for Goldman Sachs as an advisor. He sounded knowledgeable about finances. I don't know why I gave him my WhatsApp number. He started to introduce me to crypto trading. It started with small amounts. We talked about hobbies and other things. I thought he would teach me investing in Bitcoin. I started to tell him about my finances and after 3 months I had all my money invested in crypto USDT.

Finally, when I wanted to withdraw my profit, the platform was locked. They said that according to the IRS, I had to pay 22% in tax, which was more than I invested. The scammer was pretending that he was paying part of the tax for me and the rest I had to take out a loan. I reported the scammer and fraudulent website everywhere I could.

[11] This scam report was edited for brevity and clarity.

Know the red flags

Talk of trust. Scammers may spend weeks or months building a relationship with their targets. They talk about trust and its importance. This often is the first step toward asking you for money.

Unsolicited messages. If anyone reaches out to you unexpectedly, take time to verify the person and the offer. The Financial Industry Regulatory Authority's (FINRA) BrokerCheck tool allows you to verify brokers.

Promises of financial rewards with little or no risk. If the person guarantees investment returns with zero risk, it's a scam.

Offers to introduce you to cryptocurrency. If the person encourages you to take advantage of an investment opportunity such as buying cryptocurrency, take this as a huge red flag.

Insist on paying in crypto. If they insist on paying you in crypto and ask you to start an account, it's probably a scam.

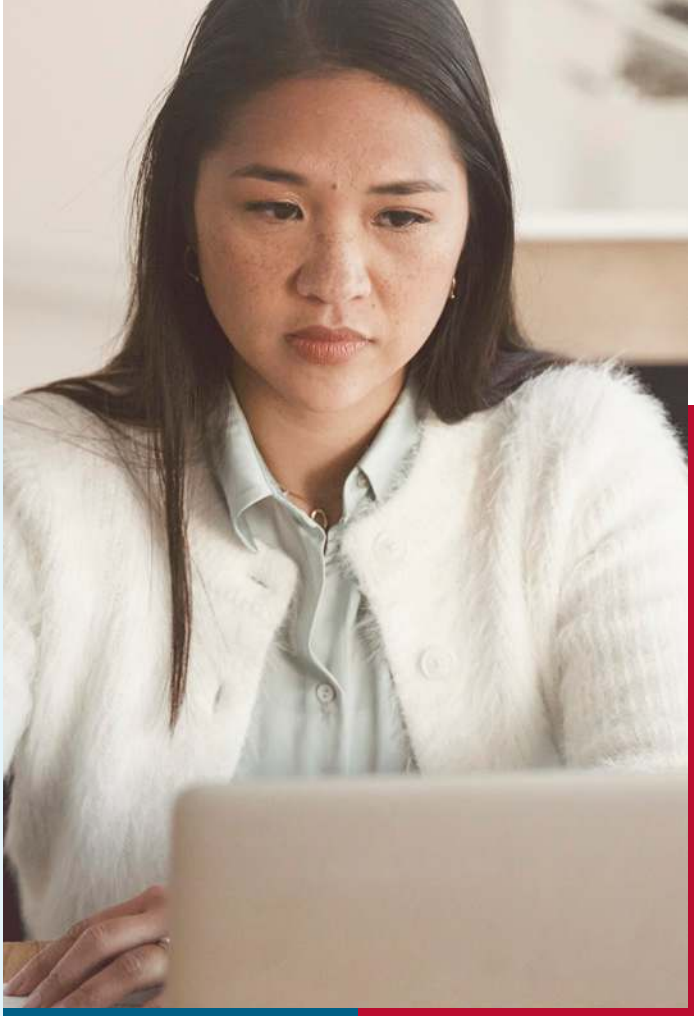
In a hurry to get off the site. Scammers will try very quickly to get you to communicate through email, messenger, or phone.

It's all moving fast. Early in the trust-building phase, scammers speak of a future together and may tell you they love you. They often say they've never felt this way before.

They are never able to meet. Be wary of someone who always has an excuse to postpone a meeting such as saying they are traveling, live overseas, or are in the military.

Using suspect language. If the person you are communicating with claims to be from your hometown but has poor spelling or grammar, uses overly flowery language, or uses phrases that don't make sense, that's a red flag.

Phishing scams rise on riskiest scams list



Phishing/social engineering scams rose from the No. 7 riskiest in 2023 to No. 6 riskiest in 2024 because of an increase in exposure and median dollar loss. Social engineering encompasses a wide range of tactics that use psychological manipulation to gain information from a person. Phishing is a type of social engineering that uses digital communications (for example, email or text message) to trick somebody into revealing sensitive information that the scammer will use to gain access to bank accounts or to steal a person's identity.

Scammers have traditionally used generic templates and information to perpetrate phishing attacks. These attempts are identifiable because they are not usually personalized to the target, and many include typos and grammatical errors. However, with more personal information being stolen from people and scammers' increased use of artificial intelligence, phishing has become much more sophisticated. Scammers can now personalize their attacks and target many more people at once.

Scammers can now personalize their attacks and target many more people at once.

The following scam report was submitted in North Carolina.[12]

The scammers sent me a letter with my personal information to claim that my home warranty was expired, and it was a final attempt to remained covered. They included my mortgage company information, though they are not affiliated with the group. Upon calling, I was told previous homeowners had paid the policy that was now expired, and as the new homeowner, I needed to provide updated information. They told me they would charge $219 monthly for 18 months and provided me with a customer service line, which is not answered and does not allow for voicemails.

Upon calling the main line again, I was told that I must have opened a policy with another group and somehow their phone number was connecting me to the wrong organization. They attempted to say they had no record of me and were in fact Omega Homecare not Superior Homecare (though the previous associate had already provided me with both of these company names). I called back again to speak with someone to cancel the plan and they continued to hang up on me.

[12] This scam report was edited for brevity and clarity.

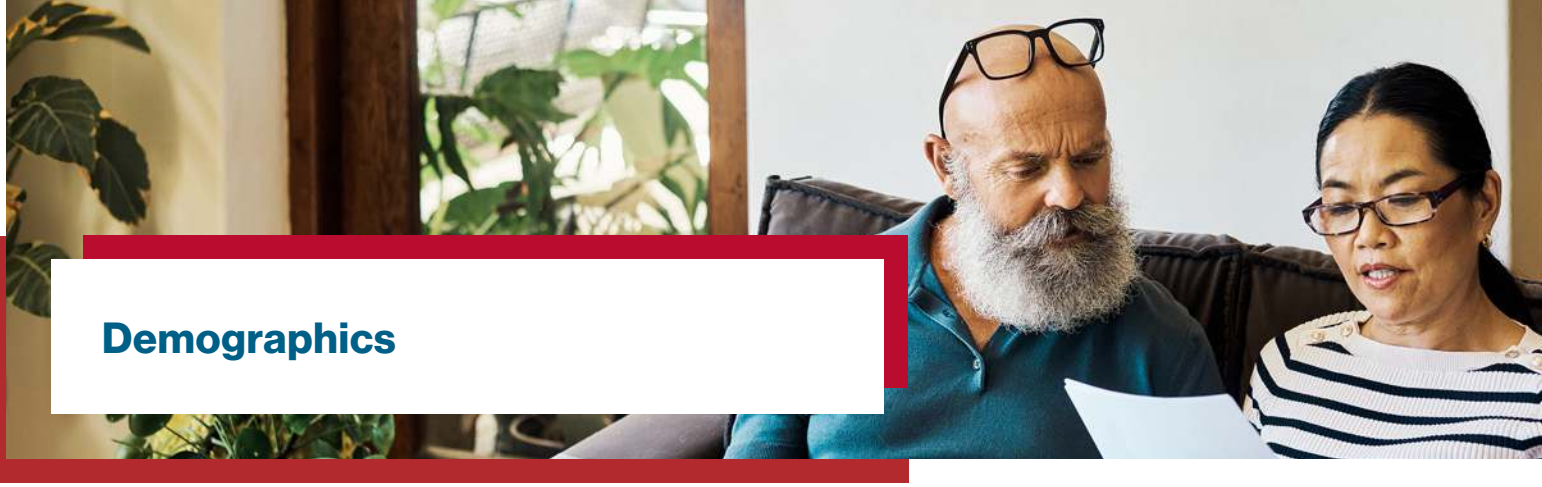
Know the red flags

Links or buttons in unsolicited messages (email, text message, etc.). Be wary of any unexpected message you receive, even if the sender claims to be somebody you trust, such as your bank or another institution. If you believe the message is legitimate, contact the business/organization directly or go to your account to confirm the details.

They ask for personal information. Always do your research before sharing any personal information with somebody, whether it is over the phone or via the internet.

They pretend to be somebody you know. Scammers may pretend to be your boss or somebody else you know to get you to share your personal information. Always double check with the person before acting.

They ask to gain access to your computer to help you fix it. Scammers pretending to be tech support people offer to fix your computer if you give them access. Once they gain access, they will steal your information and possibly download malware/ransomware onto the device. Hang up and call somebody you know and trust for help.



Demographics

Self-reported demographic data provided through BBB Scam Tracker combined with survey research helps us enhance how we target outreach and educational strategies aimed at empowering consumers and businesses to identify and avoid scams.

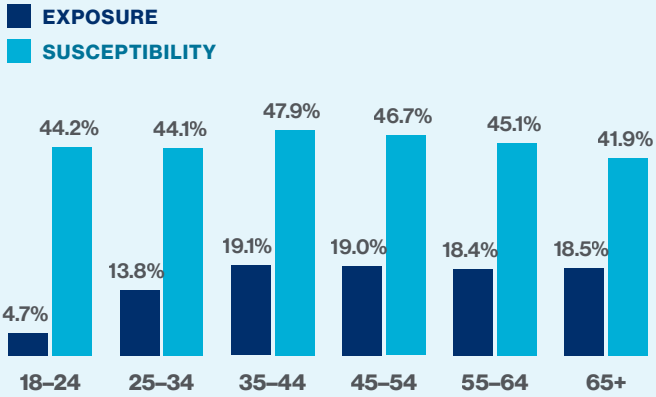
Age

This year, people ages 65+ reported the highest median dollar loss ($160), followed by people ages 18–24 ($150) (Figure 16). People ages 35–54 submitted a slightly higher percentage of reports with a monetary loss (susceptibility) than other age groups; people 65 and older reported the lowest susceptibility (41.9%).

Table 2 highlights the three riskiest scam types by age. Employment scams were the riskiest scam type for people ages 18–34. Investment/cryptocurrency scams were riskiest for those 35 years and older.

People ages 65+ reported the highest median dollar loss ($160), followed by people ages 18–24 ($150).

FIGURE 16 **Exposure, susceptibility, and median dollar loss by age (all scam types)**



The exposure for these groups does not add up to 100% because some reports did not specify age.

TABLE 2

Three riskiest scam types by age

	18–24	25–34	35–44	45–54	55–64	65+
1	Employment	Employment	Investment/ cryptocurrency	Investment/ cryptocurrency	Investment/ cryptocurrency	Investment/ cryptocurrency
2	Online purchase	Investment/ cryptocurrency	Employment	Employment	Employment	Romance/ friendship
3	Investment/ cryptocurrency	Online purchase	Romance/ friendship	Romance/ friendship	Romance/ friendship	Home improvement

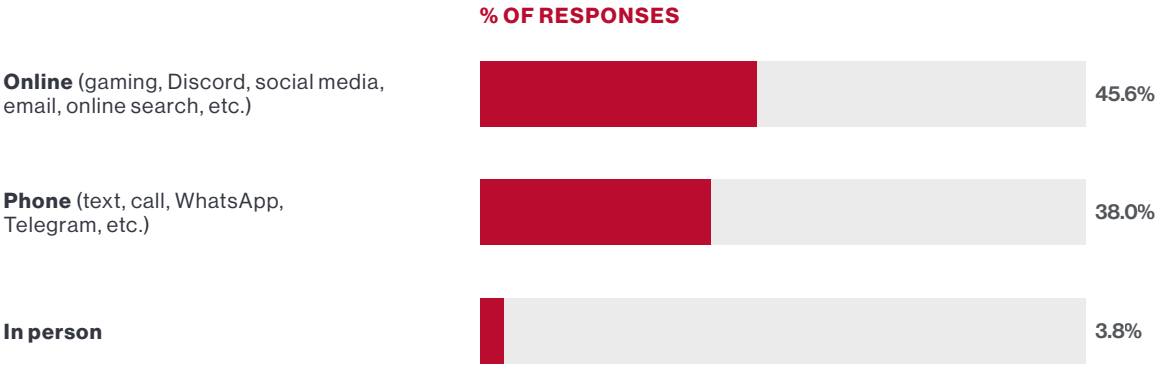
Scams targeting youth

BBB Scam Tracker does not collect information from people younger than age 18. However, we know young people are being targeted. Of the 22.9% of survey respondents who reported having children younger than eighteen, 9.7% said their children were targeted by scams. Respondents reported that their children were targeted via social media, phone call/ text message, gaming platforms, email, and phone app (Figure 17).

FIGURE 17

Reported method of contact for youth

Respondents were asked where their children first engaged with the scammer.



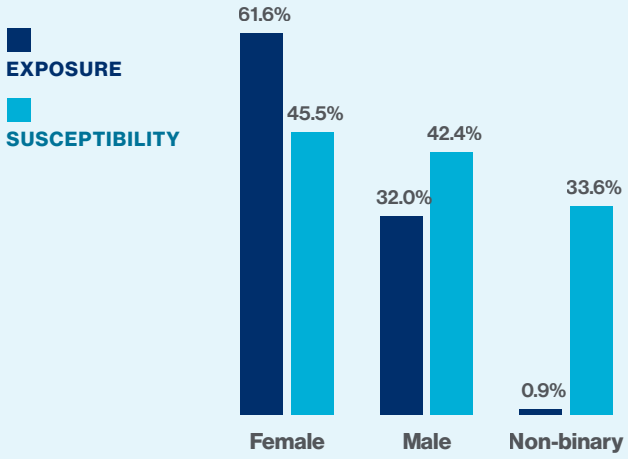
The percentages do not add up to 100% because "other" was not included.

Gender

Similar to previous years, more than 60% of reports to BBB Scam Tracker were submitted by females (Figure 18). Females reported being more susceptible to losing money when exposed to a scam (45.5%) compared to males (42.4%) and non-binary people (33.6%). The reported median dollar loss was significantly lower for females ($102) and non-binary people ($120) than for males ($200).

Females and males reported the same top three riskiest scam types (Table 3). The No. 1 riskiest scam type reported by non-binary people was employment scams.

FIGURE 18 Exposure, susceptibility, and median dollar loss by gender



The exposure for these groups does not add up to 100% because some reports did not specify gender.

TABLE 3 Three riskiest scam types by gender

	FEMALE	MALE	NON-BINARY
1	Investment/ cryptocurrency	Investment/ cryptocurrency	Employment
2	Employment	Employment	Phishing/ social engineering
3	Romance/ friendship	Romance/ friendship	Online purchase

Contact methods

Scammers most frequently used emails, phone calls, and websites to contact people according to 2024 reports. The top methods resulting in a reported monetary loss across all scam types were social media, website, and email (Figure 19).

About 82% reported losing money when they engaged with the scammer via social media, followed by those who engaged by website (79.7%) and in person (73.2%).

Median dollar loss for internet messaging rises

Those who reported losing money when contacted via internet messaging rose from 59.9% in 2023 to 68.9% in 2024. Also, the reported median dollar loss rose from $650 in 2023 to $1,000 in 2024.

Online scams

Scams perpetrated online were riskier and more likely to result in a monetary loss than were those perpetrated in person or via phone (Figure 20).

Figure 21 shows age range and contact method. Older people were more likely to report losing money when targeted by phone, online classifieds, and in person.

Online purchase scams were the most reported scam type in which the person reported engaging with a scammer via website, social media, and online classifieds (Table 4). Employment scams were the most reported scam via internet messaging, email, and text message.

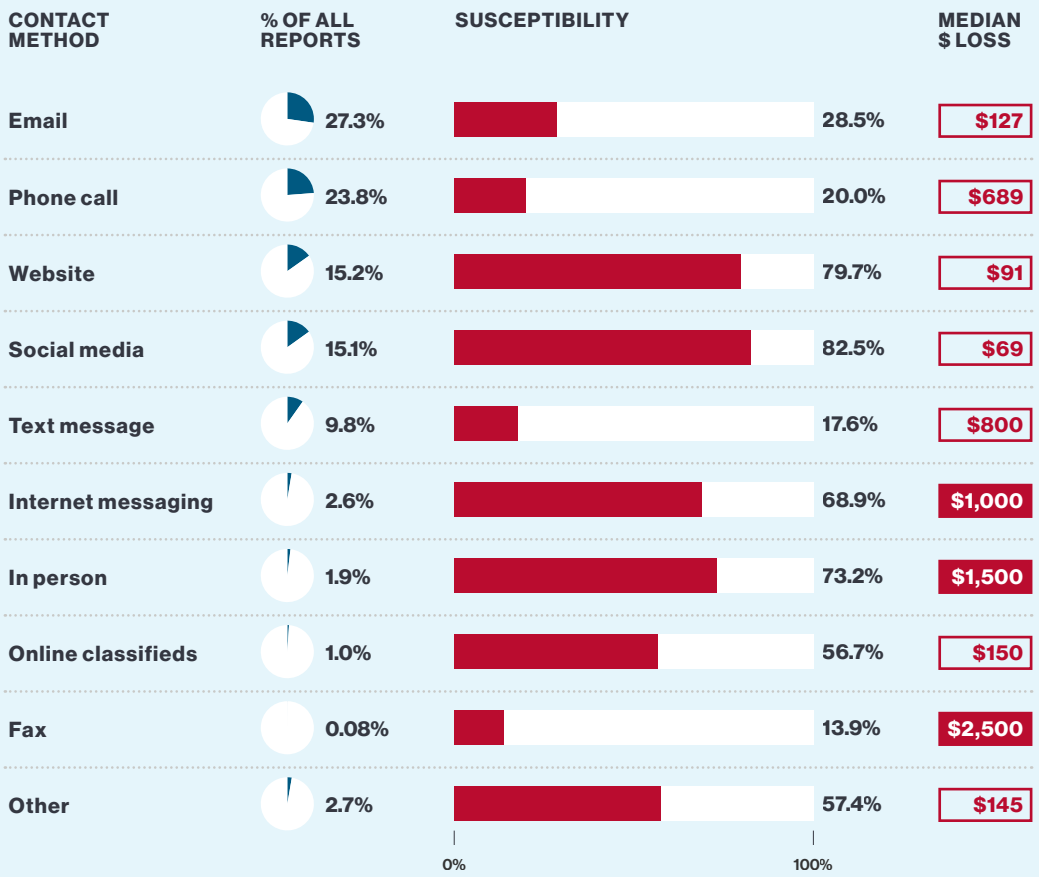
Social media scams perpetrated primarily via ads

About 36% of survey respondents[13] said the scam incident they reported involved social media. Almost 50% of scams perpetrated via social media began when the person responded to a social media advertisement or post (Figure 22). About 15% of respondents reported that the scammer sent them a direct message on a social media platform.

[13] A survey was distributed to those who submitted a scam to BBB Scam Tracker in 2024; 3,300 respondents completed the survey.

FIGURE 19

Contact method with a monetary loss



These figures do not add up to 100% because data that was "not applicable" was not included.

FIGURE 20

All scams compared to scams with a reported monetary loss by means of contact

Online

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

61.2%

of all scams reported

78.0%

of all scams reported with a $ loss

Phone

(includes phone, text message, and fax)

33.7%

of all scams reported

14.6%

of all scams reported with a $ loss

In person

(includes in person and postal mail)

1.9%

of all scams reported

3.1%

of all scams reported with a $ loss

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

FIGURE 21 Contact method by age (reports with a monetary loss)

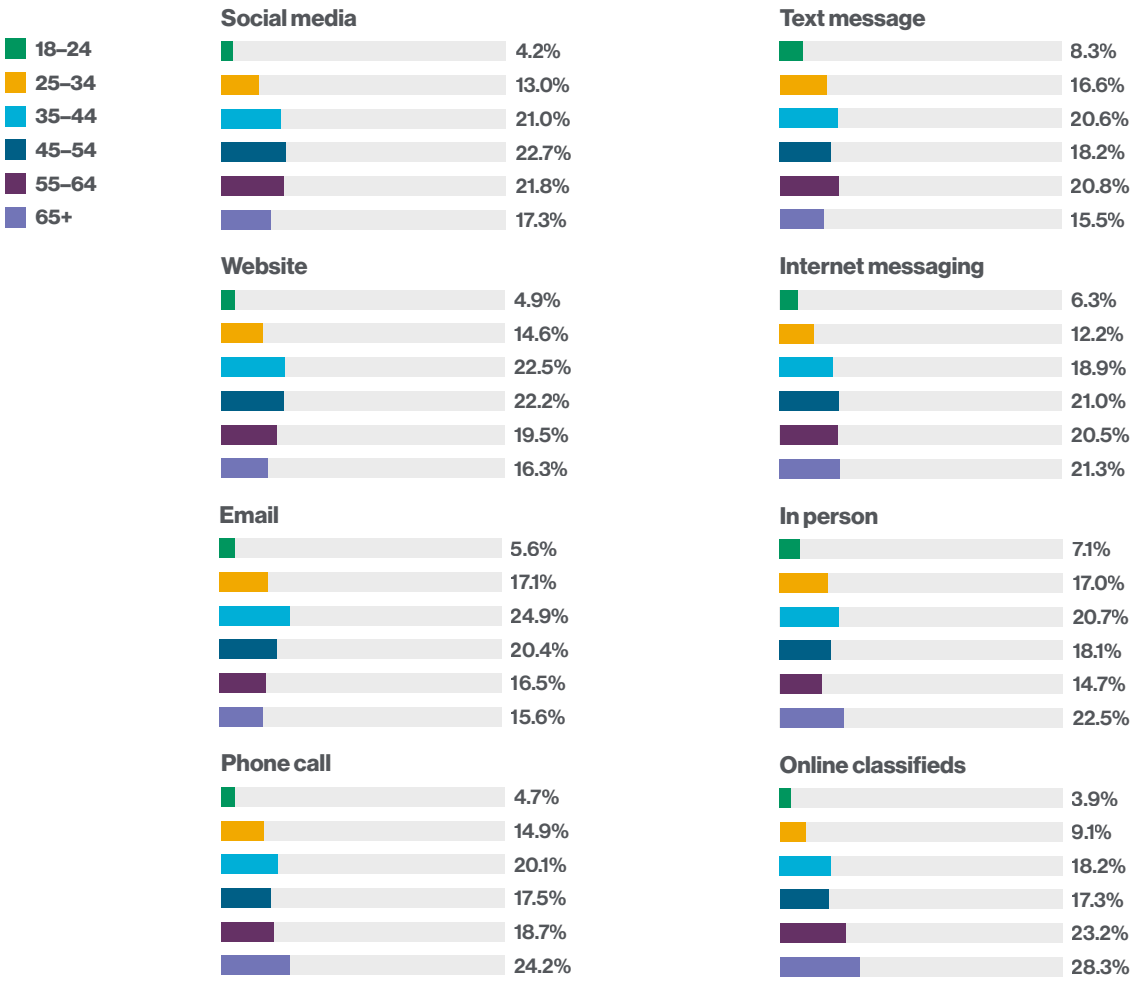
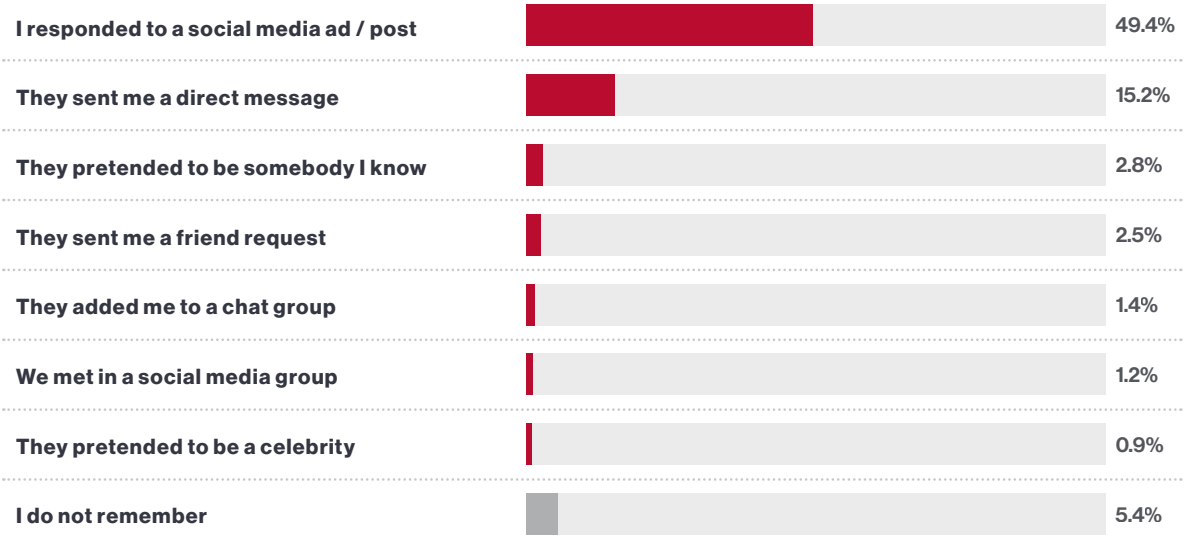


TABLE 4 Most reported scam types by contact method

CONTACT METHOD	#1	#2	#3
Website	Online purchase	Employment	Counterfeit product
Social media			
Internet messaging	Employment	Online purchase	Investment/ cryptocurrency
Online classified	Online purchase	Employment	Phishing/social engineering
Email	Employment	Online purchase	
Text message		Phishing/social engineering	Online purchase
In person	Home improvement	Retail business imposter	Utility
Phone call	Phishing/social engineering	Debt collection	Employment

FIGURE 22

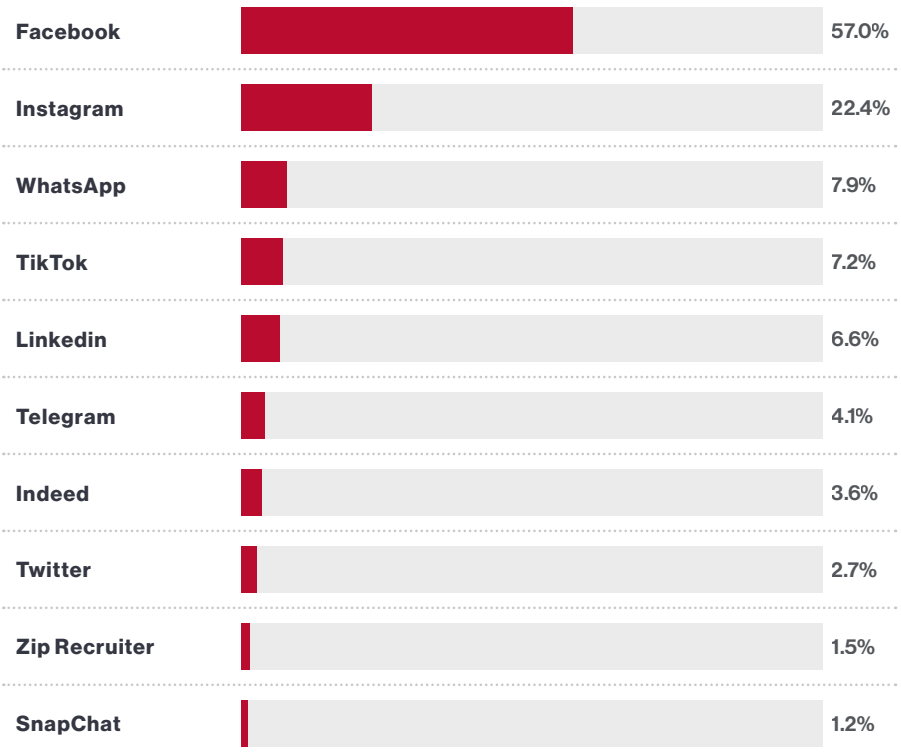
How did you engage with the scammer on social media?



The responses do not add up to 100% because the "other" category was not included.

FIGURE 23

Top reported online platforms



Responses do not add up to 100% because respondents were asked to select "all that apply."

Payment methods

Credit cards remained the top reported payment method for scams with a monetary loss (Figure 24), followed by bank account debit and online payment system (digital payment app). Payment methods with the highest median dollar loss were wire transfer, cryptocurrency, and check.

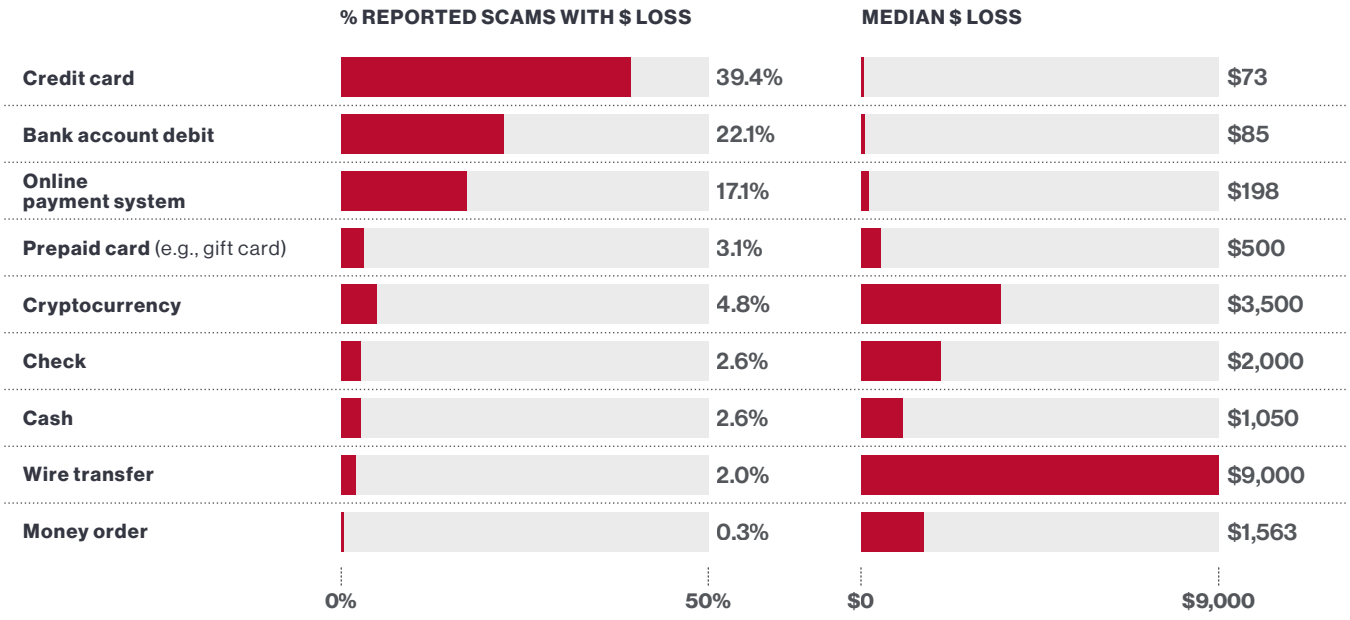
Rising impact of cryptocurrency

Reports of people paying scammers in cryptocurrency rose from 3.0% in 2023 to 4.8% in 2024. The reported median dollar loss also rose from $3,300 to $3,500.

When monetary loss is broken out by age and payment method (Figure 25), older people were more likely to report a monetary loss via prepaid/gift card and check.

Online purchase scams were the most reported scam type for several payment methods (credit card, online payment system, bank account debit, prepaid card, and wire transfer) (Table 5).

FIGURE 24 **Payment method with a reported monetary loss**



The totals do not add up to 100% because the "other" category was not included.

FIGURE 25 **Payment method by age (reports with a monetary loss)**

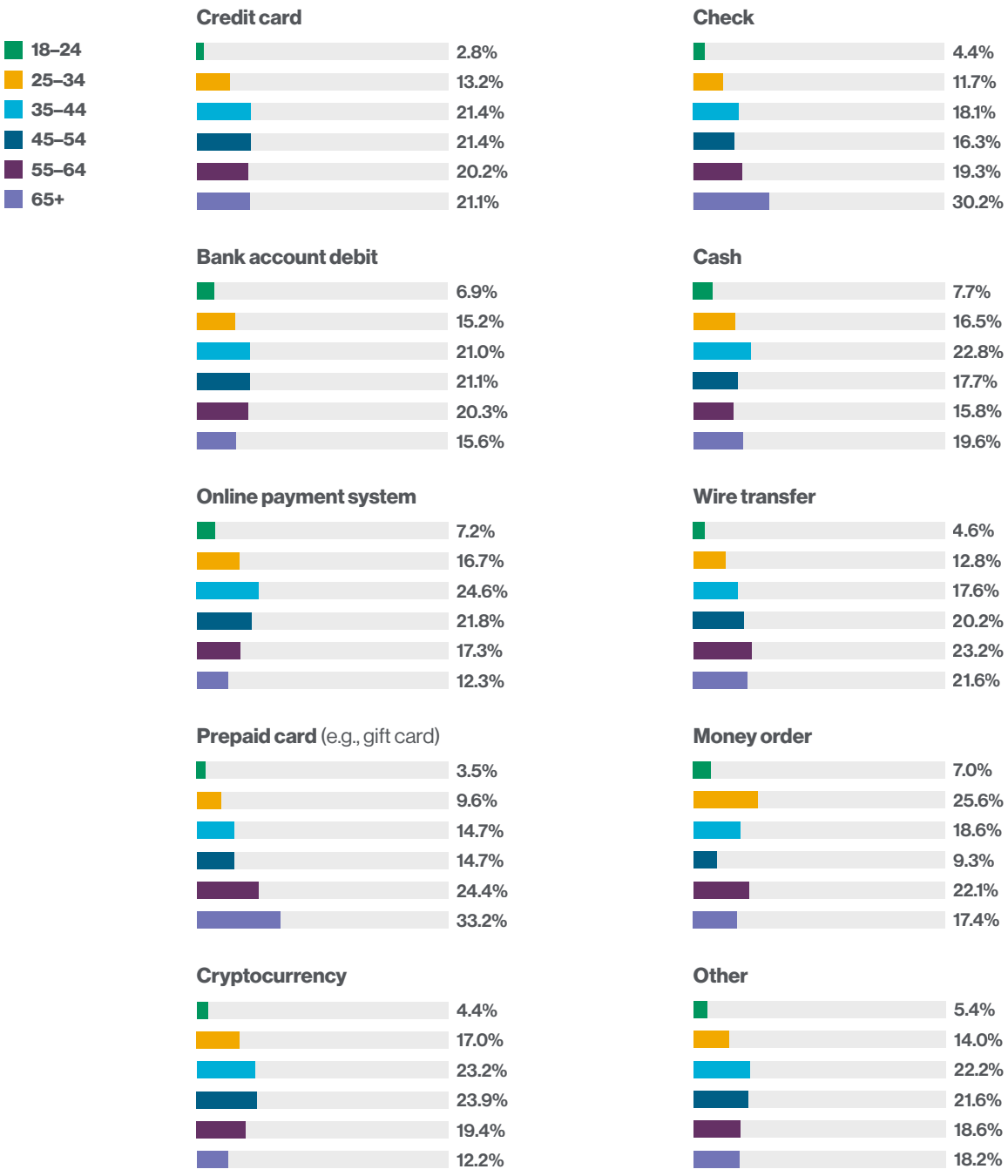


TABLE 5 Most reported scam type by payment method

PAYMENT METHOD	#1	#2	#3
Credit card	Online purchase	Counterfeit product	Travel/vacation/ timeshare
Online payment system			Employment
Bank account debit		Phishing/social engineering	
Prepaid card			Sweepstakes/ lottery/ prizes
Cryptocurrency	Investment/ cryptocurrency	Employment	Online purchase
Check	Home improvement		
Wire transfer	Online purchase	Investment/ cryptocurrency	Advance fee loan
Cash	Home improvement	Online purchase	Employment

Impact on specific audiences

Canadian consumers

In 2024, Canadian consumers reported 2.8% of total scams submitted to BBB Scam Tracker. The overall median dollar loss reported in 2024 was CAN$311, up from CAN$300 in 2023. The percentage of those who reported losing money after being targeted by a scam (susceptibility) decreased slightly from 61.1% in 2023 to 59.5% in 2024.

The top three riskiest scams reported in Canada remained the same in 2024 as those reported in 2023. Investment/cryptocurrency scams remained the No. 1 riskiest scam, with a high median dollar loss (CAN$5,000). More than 87% of those who reported being targeted by this scam type lost money (Figure 26).

Employment scams remained No. 2 riskiest, with a median dollar loss of CAN$2,500. Home improvement scams, again No. 3 riskiest, had a reported median dollar loss of CAN$1,500 and a high percentage of reports with a dollar loss (83.9%). You can view the full Canada Risk Report at BBBMarketplaceTrust.org/CanadaRiskReport.

FIGURE 26 **Top three riskiest scams reported in Canada**

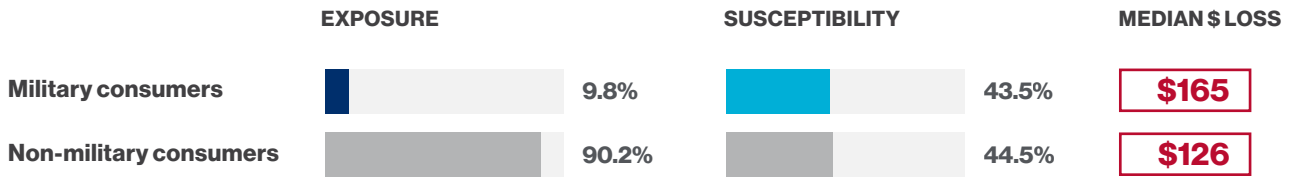
RANK	SCAM TYPE	BBB RISK INDEX	EXPOSURE / SUSCEPTIBILITY	MEDIAN $ LOSS (CAN)
1	Investment/ cryptocurrency	796.6	5.7% / 87.5%	$5,000
2	Employment	366.3	16.7% / 27.3%	$2,500
3	Home improvement	356.3	8.8% / 83.9%	$1,500

* *Exposure is limited by the nature of self-reporting; the percentage of those who reported to BBB Scam Tracker does not necessarily match the percentage of people in the full population who were targeted by scams.*

Military consumers

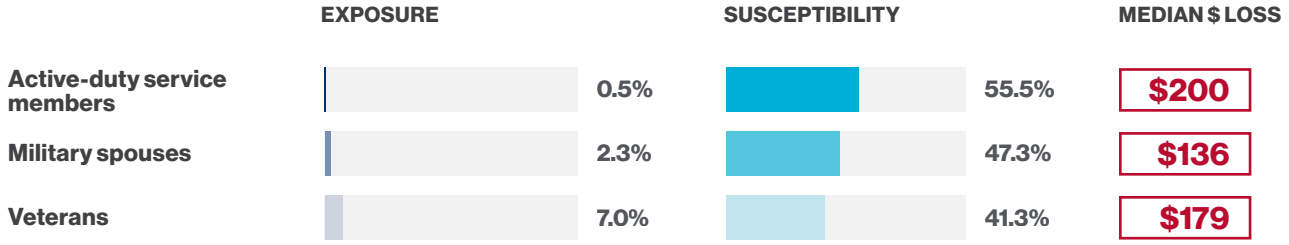
Military consumers who self-identified as being active-duty military personnel, military spouses, or veterans submitted 9.8% of all reports to BBB Scam Tracker in 2024. Military consumers reported higher median financial losses ($165) than non-military consumers ($126) (Figure 27). A slightly higher percentage of non-military consumers (44.5%) than military consumers (43.5%) reported losing money when targeted by a scam.

FIGURE 27 **Exposure, susceptibility, median $ loss (military consumers versus non-military consumers)**



As in previous years, we received more reports from veterans than from military spouses and active-duty service members. Service members submitted a higher percentage of reports with a dollar loss (55.5%) and a higher median dollar loss ($200) than veterans and military spouses (Figure 28).

FIGURE 28 **Exposure, susceptibility, median $ loss (service members, spouses, veterans)**



The BBB Risk Index was applied to identify the three riskiest scams for military spouses and veterans (Table 6). The No. 1 riskiest scam type for military spouses was employment scams. Investment/cryptocurrency scams were riskiest for veterans.

TABLE 6

Riskiest scam types: military spouses, veterans and non-military consumers

RANK	Military spouses	Veterans	Non-military consumers
1	Employment	Investment/ cryptocurrency	Investment/ cryptocurrency
2	Online purchase	Employment	Employment
3	Sweepstakes/ lottery/prizes	Home improvement	Romance/friendship

The riskiest scams for service members is not included because of a low number of reports. You can learn about the riskiest scams reported by service members in BBB Institute's 2024 report, Marketplace Challenges Facing the Military Community.

Scams targeting businesses

BBB Scam Tracker also collects information about scams that target businesses. Businesses reported losing money 29.0% of the time when they were targeted, a significantly lower susceptibility than that reported by consumers (44.4%). However, the overall median dollar loss reported by businesses, about $1,200, was significantly higher than that reported by consumers ($130) (Figure 29).

The three riskiest business scams based on the BBB Risk Index were online purchase, phishing/social engineering, and fake invoice/supplier bill scams (Figure 30).

FIGURE 29 **Susceptibility and monetary loss resulting from scams reported by businesses**

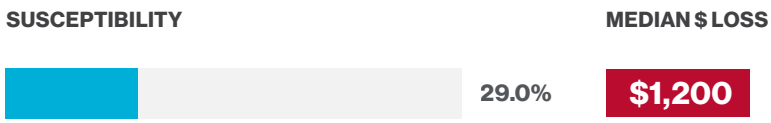


FIGURE 30 **Riskiest scam types reported by businesses**

RANK	SCAM TYPE	BBB RISK INDEX	SUSCEPTIBILITY	MEDIAN $ LOSS
1	Online purchase	79.6	56.1%	$1,000
2	Phishing/social engineering	15.0	11.2%	$1,100
3	Fake invoice/ supplier bill	9.6	14.5%	$584

Most impersonated organizations

By pretending to be well-known companies, government agencies, or organizations, scammers seek to co-opt the trust and authority of these brands. In some cases, scammers impersonate real-life individuals. In 2024, Publishers Clearing House (PCH) rose to the top of the list of most impersonated organizations reported to BBB Scam Tracker (Table 7). Although this company has been in the top three most impersonated companies since 2018, this is the first time it landed at No. 1. The U.S. Postal Service, the most impersonated organization in 2023, dropped to No. 2 on the list.

Contact methods. About 90% of Publishers Clearing House (PCH) impersonation scams were perpetrated via phone; 10% were perpetrated via email. U.S. Postal Service impersonation scams were mostly perpetrated via text message (92%); 8% were perpetrated via phone. Almost 90% of PayPal impersonation scams were perpetrated via email; 10% were perpetrated via phone. Amazon impersonation scams were perpetrated in several different ways: email (40%), phone (18%), social media (13%), text message (16%), and website (13%).

Scam types. More than 75% of Publishers Clearing House impersonation scams were sweepstakes/lottery/prize scams. Scams impersonating the U.S. Postal Service included phishing (66%) and government agency imposter (18%). PayPal impersonations included phishing (41%), bank/credit card imposter (18%), and investment/cryptocurrency (7%). Amazon impersonations primarily included phishing (36%), online purchase (17%), and retail business imposter scams (14%).

TABLE 7 **Top organizations/brands used for impersonation**

2024 Rank	2023 Rank	Organization name	No. of reports
1	3	Publishers Clearing House	572
2	1	U.S. Postal Service	515
3	6	PayPal	508
4	2	Amazon	466
5	17	Spectrum	298
6	8	Walmart	297
7	5	Norton	262
8	4	Geek Squad	192
9	7	Microsoft	190
10	14	Medicare	185
11	9	Facebook	183
12	15	Advance America	180
13	10	McAfee	165
14	11	Better Business Bureau®	142
15	NA	Apple	135
16	16	Macy's	130
17	19 / NA /NA	Tied: Capital One / Costco / Geek Tech	122
18	NA	Bank of America	111
19	NA	Wayfair	108
20	NA	Wells Fargo	104

NA = Did not appear on the list in 2023.

Other impersonation trends

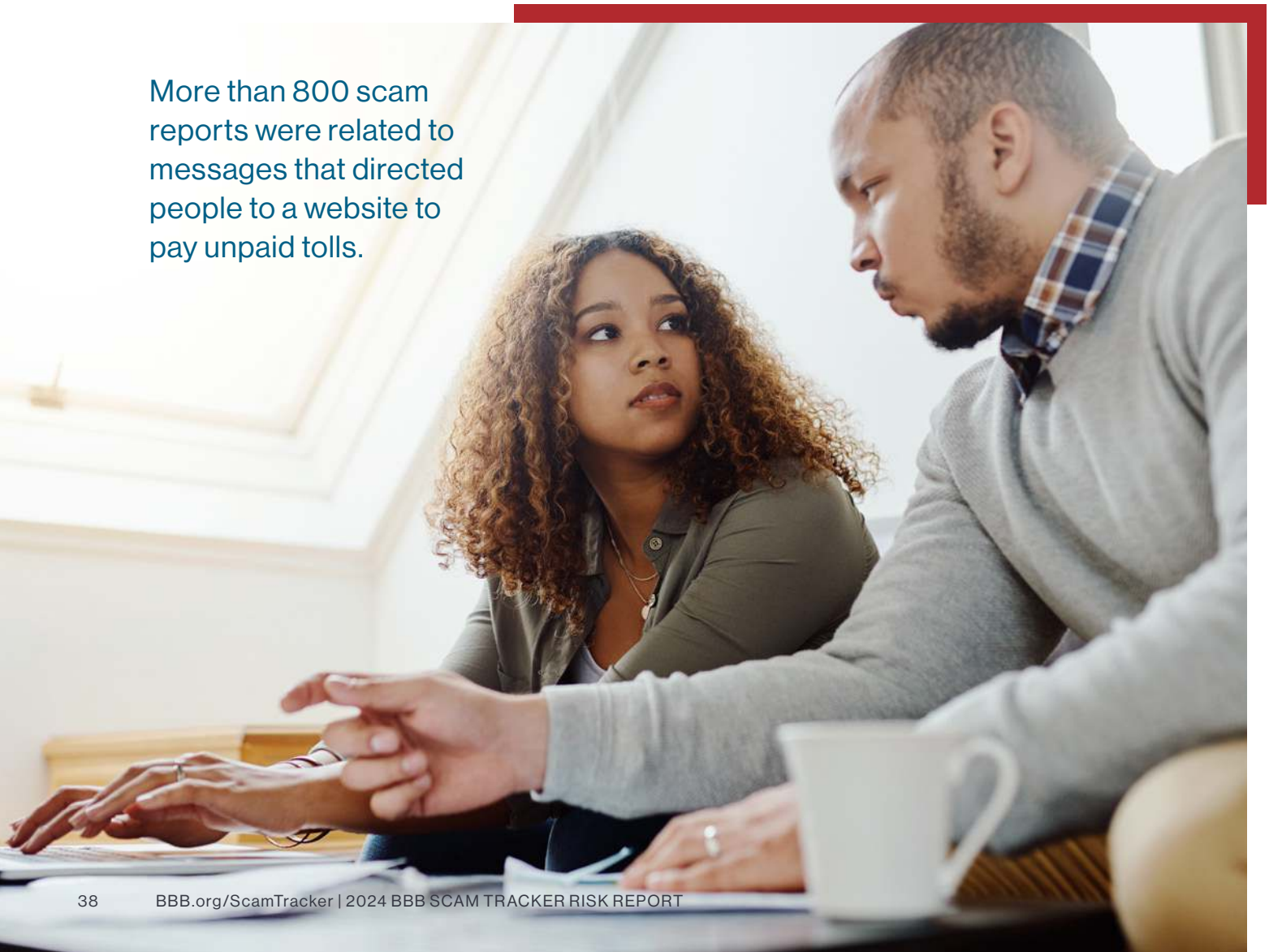
Impersonation scams can take many forms, and scammers constantly change their tactics to surprise their targets. In our data analysis, we found a few new impersonation tactics used in 2024.

Toll services. More than 800 scam reports were related to messages that directed people to a website to pay unpaid tolls.

Home warranties. A significant number of impersonation scams pretended to be home warranty businesses claiming the person's warranty expired and seeking money and/or personal information.

Court documents. Other common impersonation tactics included messages from process servers telling the person to call them back immediately to be served court documents.

Funeral expenses. We received several reports about phone calls offering final expense life insurance policies to cover funeral costs.

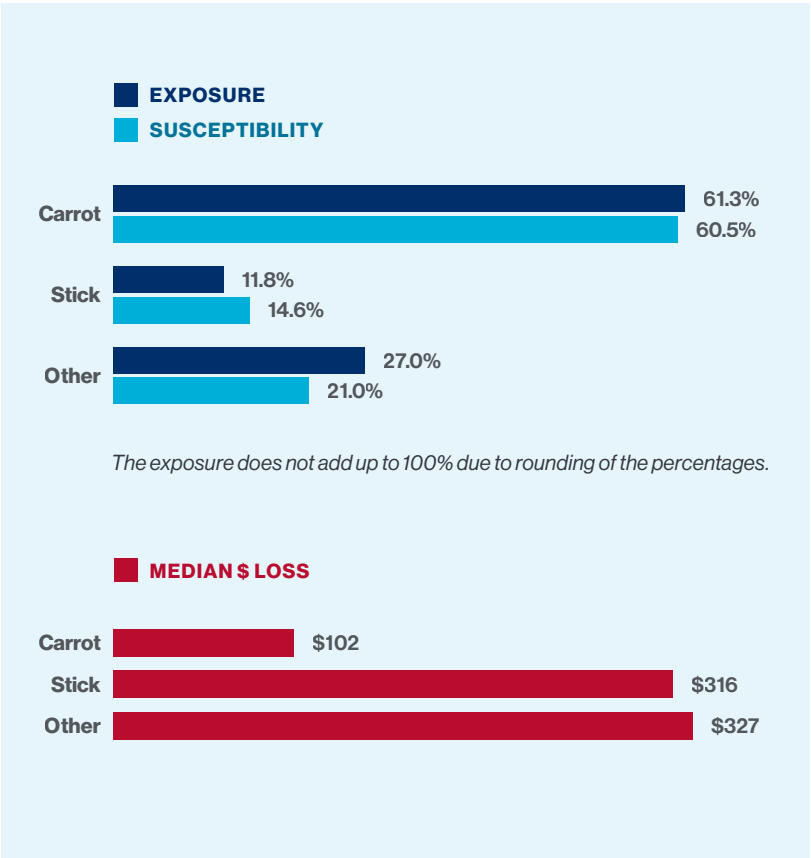


Carrot versus stick: Analyzing the impact of scam tactics

Scammers use a wide variety of tactics, some more effective than others. Some tactics use the promise of an opportunity ("carrot") to encourage the target to continue the engagement. Examples of the carrot approach include the chance to make quick money through low-risk investments or too-good-to-be-true job offers. Other tactics utilize a threat ("stick") or negative situation to manipulate the targets, such as jail time for back taxes or news that a loved one is in trouble and needs help.[14] In Figure 31, the various scam types are divided into three categories: carrot method, stick method, and other (scam types that do not easily fit into a category).

Scammers were much more likely to use a carrot tactic (61.3%) to perpetrate their scams than a stick tactic (11.8%) (Figure 31). However, when people reported losing money to scams that were perpetrated with

FIGURE 31 **"Carrot" versus "Stick" tactics by exposure, susceptibility, and median dollar loss**



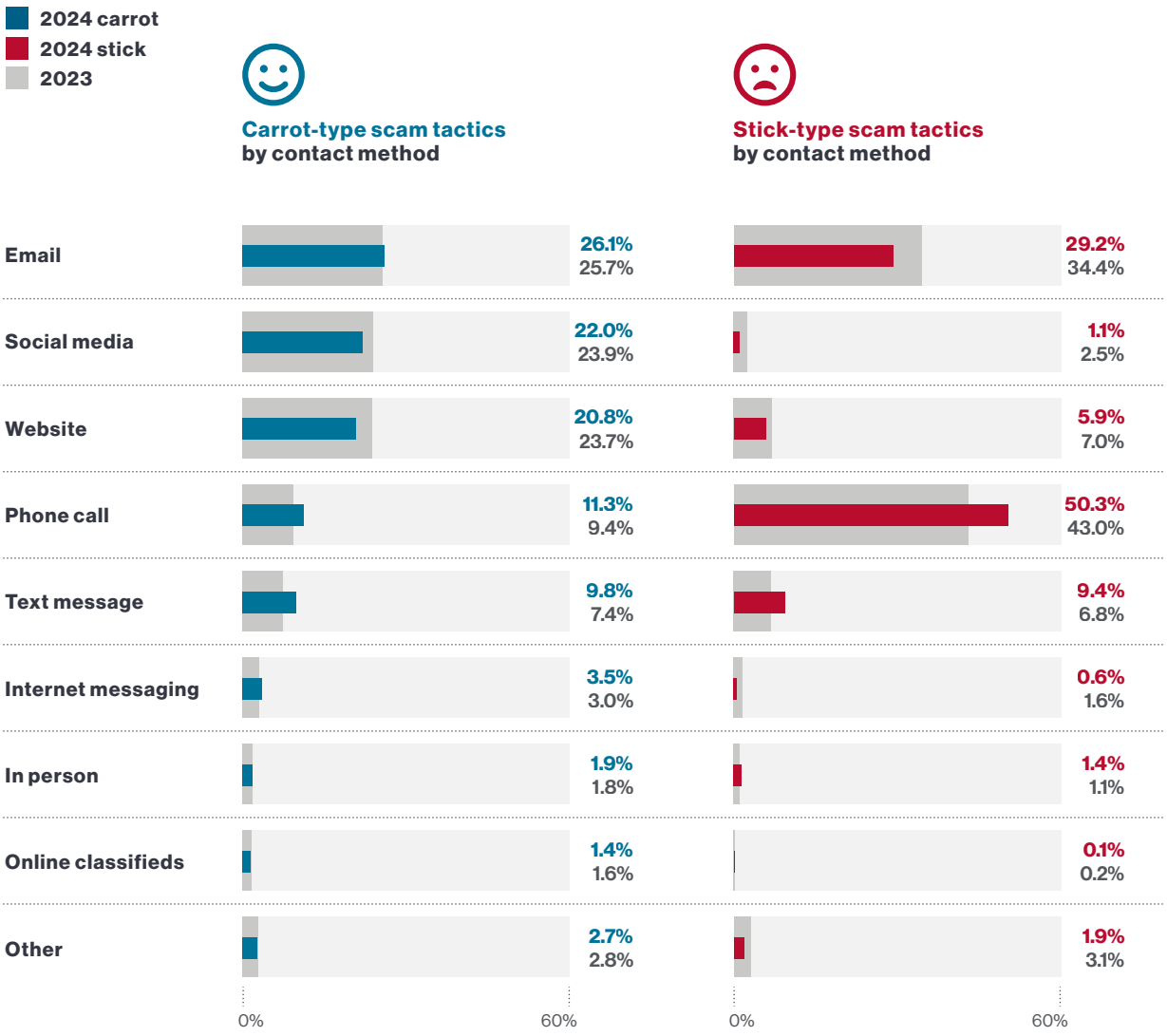
[14] Scams targeting both consumers and businesses were included in this analysis. The breakdown of scam types includes the following:

- **Carrot scams:** Advance fee loan, investment/cryptocurrency, fake check/money order, credit repair/debt relief, employment, counterfeit product, government grant, home improvement, sweepstakes/lottery/prizes, charity, foreign money exchange, rental, romance/friendship, vanity award, travel/vacation/timeshare, online purchase, Yellow Pages/directories, worthless problem-solving service, and retail business impersonation.
- **Stick scams:** Debt collection, tax collection, business email compromise, family/friend emergency, government agency imposter, fake invoice/supplier bill, tech support, and utility.
- **"Other" scams that don't easily qualify as carrot or stick:** Phishing, bank/credit card company imposter, identify theft, credit card, moving, and healthcare/Medicaid/Medicare.

a stick method, they reported losing significantly more money ($316) than those who reported losing money to carrot-type scams ($102).

Carrot-type tactics were more likely to use social media or websites to target people. Stick-type tactics were more likely to target people via phone (Figure 32). Interestingly, carrot-type tactics via text message rose from 7.4% in 2023 to 9.8% in 2024; stick-type tactics via text message also rose, from 6.8% to 9.4%. Stick-type tactics via phone call increased from 43.0% in 2023 to 50.3% in 2024.

FIGURE 32 **Contact method by carrot or stick method**

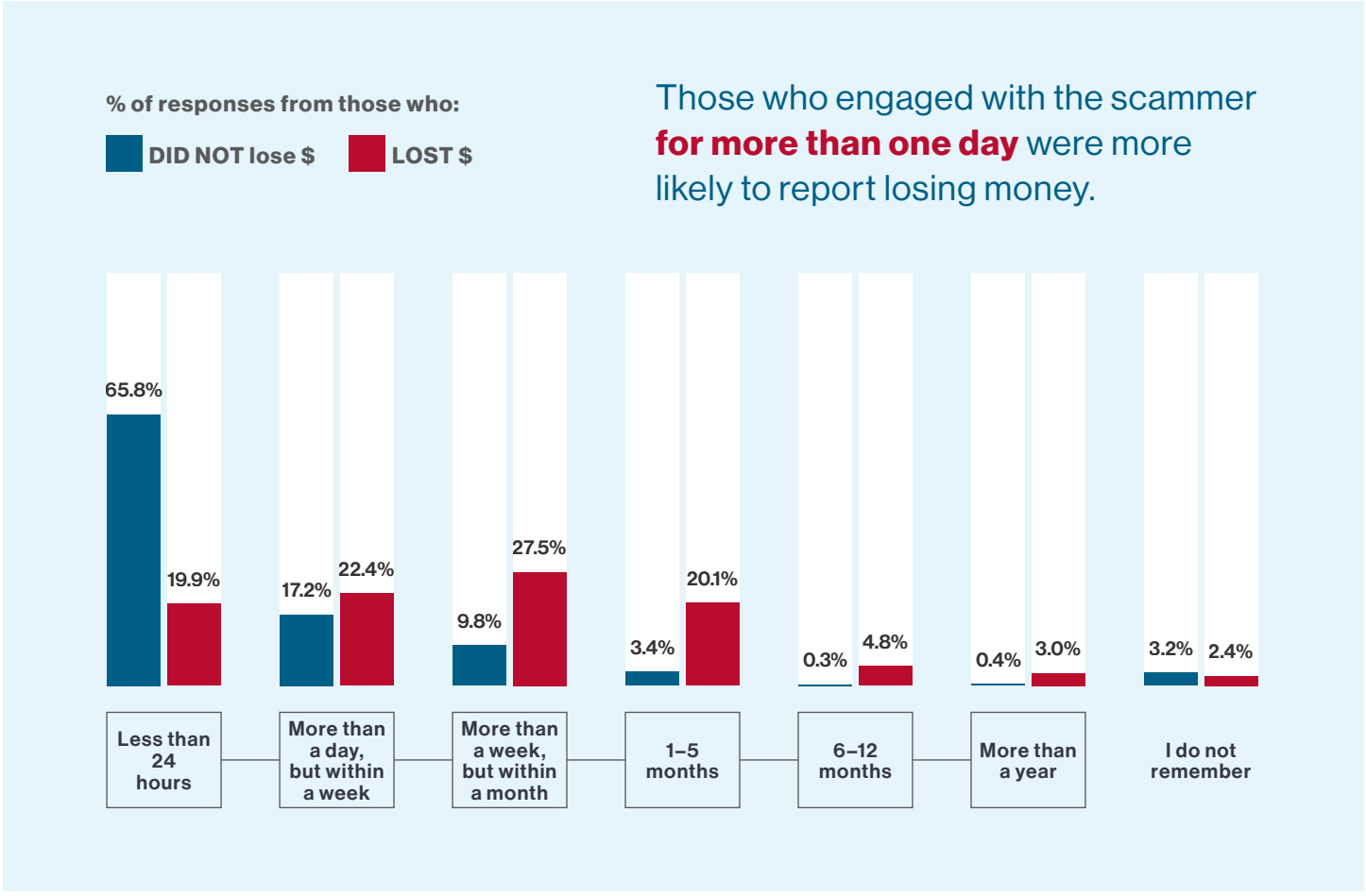


Percentages do not add up to 100% because data that was "not applicable" was not included.

Identifying scams in the marketplace

Scams have become more sophisticated and difficult to spot. The three riskiest scams on our list all typically involve building trust with targets before the fraud occurs. We asked survey respondents how long it took them to realize the incident was a scam (Figure 33). Those who engaged with the scammer for more than one day were more likely to report losing money.

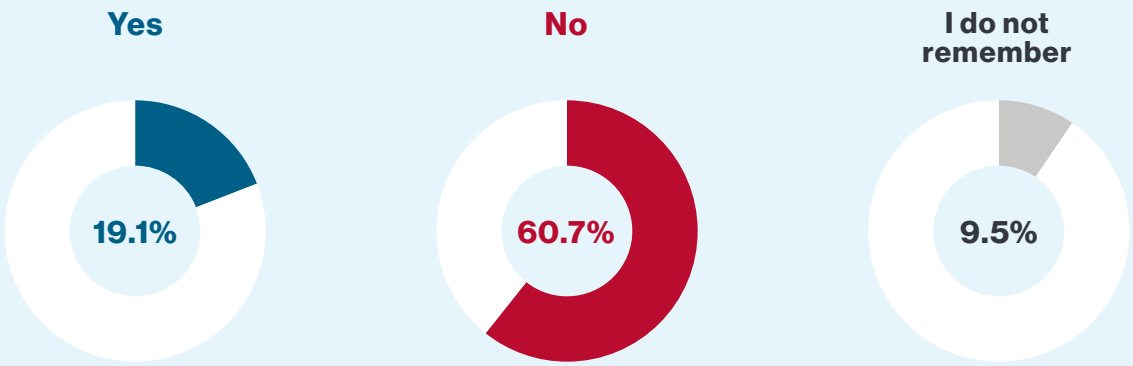
FIGURE 33 **How long did you interact with the scammer before you suspected it was a scam?**



Gifts cards and third-party interventions

Scammers continue to urge victims to pay them with gift cards because they can be non-traceable. Like the previous year, 3.1% of scams with a dollar loss were paid with gifts cards. The median dollar loss for this payment method was $500. Some banks, retailers, and other businesses are beginning to train their employees to speak up if they see somebody buying multiple prepaid cards/gift cards. About 19% of survey respondents said a store employee warned them that the situation might be a scam (Figure 34).

FIGURE 34 **When you purchased the card(s), did a store employee say anything about the situation being a possible scam?**



The responses do not add up to 100% because the "not applicable" category was not included.

Other factors that may impact victimization

Repeat victimization

When we asked survey respondents to self-report how many times they lost money to a scam, 12.4% reported losing money at least three times, up from 10.3% in 2023 (Figure 35). Notably, 3.8% reported losing money five or more times, up from 2.1% in 2023.

Life changes

People who said they were either retired, lost their spouse, or went through a divorce were more likely to report losing money, according to our survey research.

Comfort with technology and online life

Younger survey respondents reported being more comfortable with technology and online life than older people. More specifically, they reported feeling more comfortable meeting new people online, allowing tech support to remotely access their computers, downloading phone apps, adding new friends on social media, sharing personally identifiable information on social media, and experimenting with new technologies.

FIGURE 35 Number of times a person reported losing money to a scam

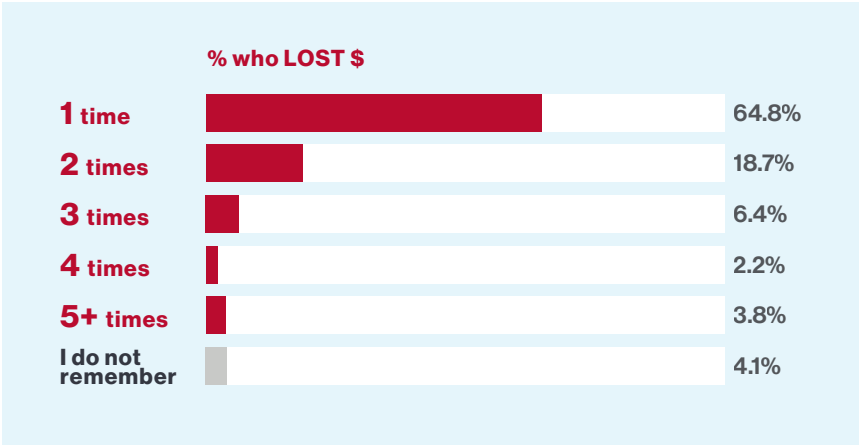
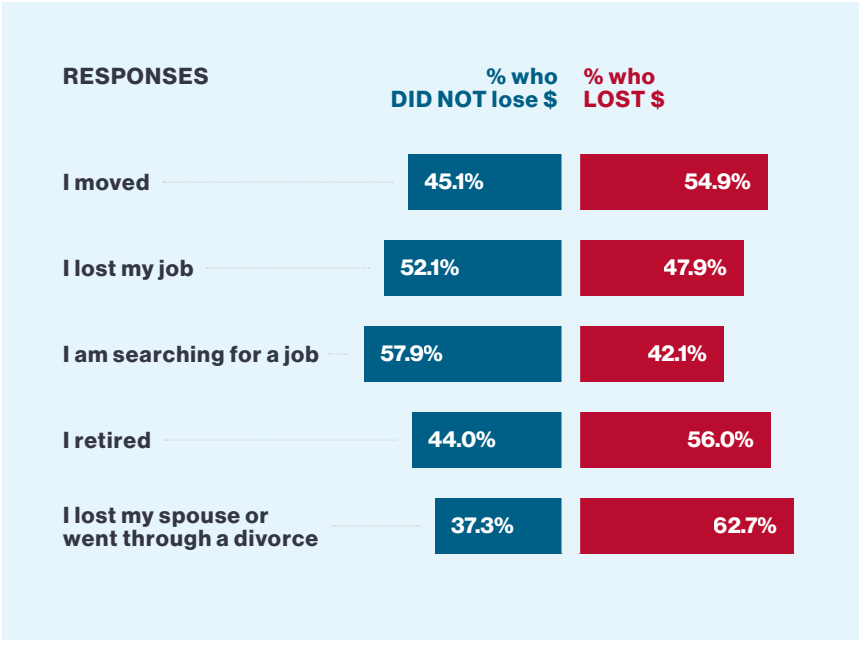
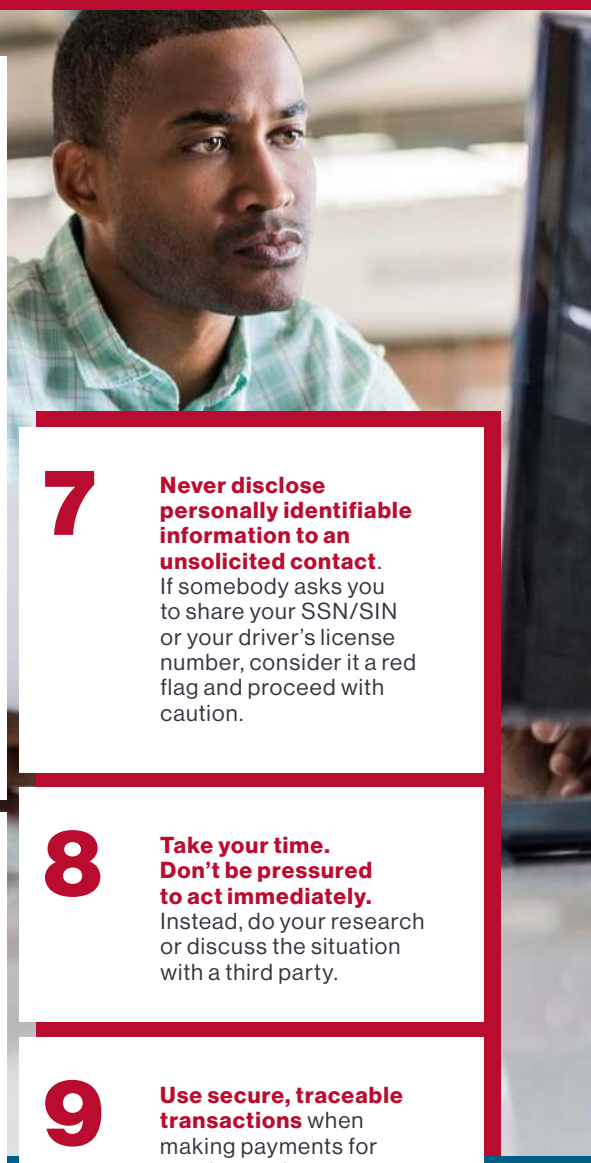


FIGURE 36 Life changes and money loss



10 GENERAL TIPS FOR AVOIDING A SCAM

These tips can help you avoid most scams and protect yourself and your family.



1 **Avoid making quick purchases while browsing social media.** Take time to research the ads that offer those great deals. Scammers advertise websites that offer great deals but either don't deliver the product at all or deliver counterfeit products.

2 **Be very cautious engaging with someone you've met online.** Make sure you don't share personal details with somebody you haven't met in person. If they begin to ask for money or offer a no-risk investment opportunity, it's a red flag.

3 **Don't click on links or open attachments in unsolicited email or text messages.** If the sender claims to be somebody you know or a well-known organization, contact the person directly or go directly to your account to confirm the details. Impersonation is a common tactic used to perpetrate scams.

4 **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.

5 **Take precautions when making online purchases.**

- Don't shop based 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 ***s*** is for "secure") and a small lock icon on the address bar. However, even secure websites can be fraudulent.
- Do more research on the products and the business before you make the purchase.

6 **Know general red flags of scams:**

- The offer sounds too good to be true.
- The person insists you must act immediately, or the deal ends soon.
- Somebody asks you to deposit money into a Bitcoin ATM or sends a check and asks you to deposit it and then transfer the funds.
- They require an up-front payment before a service is provided.
- They ask you to continue the conversation on another communications platform.

7 **Never disclose personally identifiable information to an unsolicited contact**. If somebody asks you to share your SSN/SIN or your driver's license number, consider it a red flag and proceed with caution.

8 **Take your time. Don't be pressured to act immediately.** Instead, do your research or discuss the situation with a third party.

9 **Use secure, traceable transactions** when making payments for goods, services, taxes, and debts. Prepaid/gift cards, for example, cannot be traced. They are intended to be used as gifts, not as payment.

10 Whenever possible, **work with businesses that have proper identification, licensing, and insurance.** Research the company first at BBB.org.

Learn more about avoiding scams at **BBB.org/AvoidScams** or **BBB.org/ScamTips**

Learn more about scams targeting businesses at **BBB.org/all/business-scams**

BBB Institute for Marketplace Trust

The *BBB Scam Tracker Risk Report* is published annually by the BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the International Association of Better Business Bureaus. Our mission is to educate and protect consumers, establish best practices for businesses, and solve complex marketplace problems. Our consumer education programs, which include a wide array of resources on fraud prevention, are delivered digitally and in person through the network of BBBs serving communities across the United States and Canada. Research is an integral component of our work that enables us to incorporate the latest scam trends in our consumer education resources and initiatives. You can find more information about BBB Institute and its programs at BBBMarketplaceTrust.org.

Scam Prevention Guide

In 2023, BBB Institute launched our Scam Prevention Guide to help people learn how to spot and avoid scams. The guide includes quizzes, videos, a library of materials, and a Risk Calculator that helps users understand the types of scams that pose the biggest risk to their demographic profile (age, gender, country, military status). You can find the guide at BBB.org/ScamPrevention.

Scam Survival Toolkit

In 2024, we introduced a new online resource for scam survivors. The Scam Survival Toolkit connects scam victims with the resources they need to restore their financial, mental, and emotional well-being. Visit BBB.org/ScamSurvivalKit.

BBB Institute research

Marketplace challenges facing the military community

BBB Institute partnered with the Association of Military Banks of America (AMBA) and Zelle® to publish a new report in 2024, *Marketplace challenges facing the military community*. This report highlights the ways in which unique challenges affect how military consumers engage in the marketplace. Download the report at BBBMarketplaceTrust.org/MilitaryResearch.

Thank you to our sponsors.

BBB Institute would like to recognize our funding partners for making BBB Institute's research and programs possible.

amazon

BBB

CapitalOne

FINRA Investor Education FOUNDATION

PayPal

Walmart

See all BBB Institute research at BBBMarketplaceTrust.org/research

GASA SCAMADVISER

Best Scam Fighting Tool 2024

Award Winner

Voted the Best Scam Fighting Tool

by the Global Anti-Scam Alliance and ScamAdviser.com

Learn more about BBB Scam Tracker:

BBB.org/ScamTracker

Acknowledgements

BBB Scam Tracker relies on the trust of the 112-year-old BBB brand to collect data from people who have been targeted by fraudsters. The program is made possible thanks to the dedicated collaboration of BBBs working in communities across the United States and Canada; BBBs review consumer reports to eliminate those that do not appear to be actual scams, thus ensuring the best data possible is collected.

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, BBB Serving Western Pennsylvania; Jane Rupp, president and CEO, 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; Lindsay Walsh, operations assistant, BBB Serving Vancouver Island, the Gulf Islands, Haida Gwaii Powell River; Tricia Pazsint, director of investigations and advertising, BBB Serving Western Pennsylvania; and Josh Planos, vice president of marketing, communications, and PR, BBB Midwest Plains.

We would also like to thank the International Association of Better Business Bureaus for its support of BBB Institute and the *2024 BBB Scam Tracker Risk Report*. We extend a special thank you to IABBB chief knowledge officer Dr. Rubens Pessanha, MBA, PMP, SPHR, GPHR, SHRM-SCP and IABBB data quality analyst Ryan Hessling for analyzing the BBB Scam Tracker and survey research data for this report. We also give thanks to IABBB director of public relations and social media Melanie McGovern, IABBB director of marketing and communications Sara Grube, IABBB associate general counsel Barbara Johnson, and IABBB director of brand policy Jody Thomas for providing their insights and input and helping us share these findings with the public.

Project team

Mark Batchelor is the senior director of programs and outreach for the BBB Institute for Marketplace Trust where he oversees programming designed to educate consumers and businesses about how to identify signs of fraud and avoid scams. With more than 16 years of service in nonprofit outreach, he has tackled issues involving cybercrime, financial stability, senior services, trafficking survivors, and persons with disabilities. He is driven to help people impacted by online scams and fraud to find resources for recovery.

Ryan Hessling is a data quality analyst for the International Association of Better Business Bureaus. Coming from a career in the environmental sciences, Ryan has experience in data gathering, processing, and analysis. He enjoys how much can be learned and inferred by diving into data sets from around the world. A native of southeastern Connecticut, he has two degrees from Three Rivers Community College and a bachelor's from the University of Connecticut. During his downtime, when he is not taking a new course or working on projects, you can find him by the ocean reading a book or walking his dog.

Melissa "Mel" Lanning is the executive director of the BBB Institute for Marketplace Trust. Mel has more than 25 years of nonprofit leadership experience and has worked with a wide range of nonprofit organizations and trade associations. In addition to leading BBB Institute, Mel is the coauthor of *Marketplace Challenges Facing the Military Community* (2024), *Targeting Our Youth: How Scams Are Impacting Ages 18–24*, *Start With Trust Online: Online Scams* (2022), the *Online Purchase Scams Report* (2020 and 2021), the *BBB Scam Tracker Risk Report* (2017–2023), *Scams and Your Small Business* (2018), 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.

Dr. Rubens Pessanha, MBA, PMP, GPHR, SPHR, SHRM-SCP, a production engineer with an MBA, is the chief knowledge officer 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. He completed his doctorate at George Washington University. He is the coauthor of the *BBB Scam Tracker Risk Report* (2017–2023), *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), *Targeting Our Youth: How Scams Are Impacting Ages 18–24*, and the *BBB Industry Research Series—Airlines* (2018), among other titles. As a hobby, Rubens teaches project management, business ethics, strategy, and marketing for graduate and undergraduate students.

Jennifer "Jenn" Steiner-Kotch is the user interface/user experience (UI/UX) developer for the International Association of Better Business Bureaus. She leverages her expertise in user experience research and digital accessibility to develop human-centered and inclusive technology solutions. Jenn has a bachelor's degree from Arcadia University and a master's degree in human–computer interaction from Iowa State University. She is UX certified through Nielsen Norman Group and a Certified Professional in Accessibility Core Competencies (CPACC) through the International Association of Accessibility Professionals. Outside of work, you can often find her knitting scarves or learning American Sign Language.

APPENDIX A: Glossary of scam types

Scams reported to BBB Scam Tracker this year are classified into consumer scams and business scams. Although scams vary widely, about 95% of all scams reported to BBB Scam Tracker can be classified into one of these general types. You can find prevention tips for all these scam types at https://www.bbb.org/all/scamtips.

*The scam types **highlighted in blue** are scams that are only reported 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. Read our advance fee loan prevention tips.
BANK/CREDIT CARD COMPANY IMPOSTER	This scam typically involves impersonation of a bank or other credit card issuer. Under the guise of verifying account information, they persuade their targets to share credit card or banking information.
BUSINESS EMAIL COMPROMISE	A scammer impersonates a senior executive via email or another communication vehicle to persuade an employee to transfer payment for goods to another bank account. Read our business email compromise tips.
CHARITY	Fake or imposter charities are used 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. Read our charity scam prevention tips.
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. Read our counterfeit product scam prevention tips.
CREDIT CARD	Scammers impersonate a bank or other credit card issuer, pretending to verify account details to get a target's credit card or banking information. Read our credit card scam prevention tips.
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. Read our credit repair/debt relief scam prevention tips.
DEBT COLLECTION	Phony debt collectors harass their targets to get them to pay debts they don't owe. Read our debt collection scam prevention tips.
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. Read our employment scam prevention tips.
FAKE CHECK/ MONEY ORDER	The victim deposits a check they don't realize is fake and then returns a portion by wire transfer or digital payment app 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. Read BBB's Fake Check study.
FAKE INVOICE/ SUPPLIER BILL	Scammers target business owners and hope they won't notice a bill, often for office supplies that the company never ordered. They may even deliver unordered merchandise and then try to make the business pay. In other cases, scammers send urgent notices for renewal of website domain hosting or other critical services, hoping businesses will pay without proper due diligence. Read our fake invoice/supplier bill tips.

APPENDIX A: Glossary of scam types

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. Read our family/friend emergency scam prevention tips.
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. Read our foreign money exchange scam prevention tips.
GOVERNMENT AGENCY IMPOSTER	Scammers pretend to be representatives of a U.S. or Canadian government agency such as the IRS, the Canada Revenue Agency, the Social Security Administration, or a wide range of others. In 2024, scammers pretended to be from the U.S. Postal Service.
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. Read our government grant scam prevention tips.
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. Read our healthcare scam prevention tips.
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. Read our home improvement scam prevention tips.
IDENTITY THEFT	Identity thieves use a victim's personal information (e.g., SSN/SIN 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. Read our identity theft scam prevention tips.
INVESTMENT/ CRYPTOCURRENCY	Investment scams take many forms, but all prey on a target's 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. Read our investment scam prevention tips. Cryptocurrency 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. Read the BBB study on crypto scams.
MOVING	These schemes involve rogue moving services offering 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. Read our moving scam prevention tips.
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. Read our online purchase scam prevention tips.
PHISHING/SOCIAL ENGINEERING	In these schemes, scammers impersonate a trustworthy entity, such as a bank or mortgage company, and employ communications to mislead recipients into providing personal information that the scammer will use to gain access to bank accounts or steal recipients' identity. This type of scheme can also happen within the workplace as an email coming from the CEO, accounting department, or other member of management seeking personal information. Read our phishing scam prevention tips.

APPENDIX A: Glossary of scam types

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. Read our rental scam prevention tips.
RETAIL BUSINESS IMPOSTER	Scammers pretend to be well-known retail businesses. Oftentimes, the scammer will send an unsolicited text or email requesting that the recipient click a link to verify account details or respond to a concern about their account. The goal is to get access to the person's account.
ROMANCE/ FRIENDSHIP	An individual believing he/she is in a romantic relationship or new friendship agrees to send money, personal and financial information, or items of value to the perpetrator. Sometimes perpetrators will offer investment opportunities, such as cryptocurrency. Read our romance/friendship scam prevention tips.
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. Read our scholarship scam prevention tips.
SWEEPSTAKES, LOTTERY, AND PRIZES	Victims are told 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. Read our sweepstakes/lottery/prizes scam prevention tips.
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. Read our tax collection scam prevention tips.
TECH SUPPORT	Tech support scams start with a call or pop-up warning that alerts the target about 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. Read our tech support scam prevention tips.
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. Read our travel scam prevention tips.
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. Read our utility scam prevention tips.
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—for an up-front fee, of course.
YELLOW PAGES/ DIRECTORIES	Scammers convince a business to pay for non-existing advertising or a listing in a non-existent directory or "Yellow Pages." In some cases, the directory will technically exist, but is not widely distributed, and a listing is of little or no value.

*The scam types **highlighted in blue** are scams that are only reported by businesses.*

APPENDIX B: Scam type data table, consumer scams

SCAM TYPE	RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN $ LOSS
Advance fee loan	39.7	1.7%	30.1%	$ 1,000
Charity	1.3	0.2%	31.7%	$ 250
Counterfeit product	10.8	2.1%	80.7%	$ 84
Credit card	11.0	1.0%	28.5%	$ 500
Credit repair/debt relief	12.8	0.4%	53.9%	$ 750
Debt collection	12.1	5.4%	5.8%	$ 500
Employment	284.3	14.4%	17.2%	$ 1,500
Fake check/money order	6.0	0.3%	21.5%	$ 1,139
Family/friend emergency	6.6	0.2%	33.3%	$ 1,300
Government agency imposter	4.8	2.0%	25.9%	$ 120
Government grant	21.7	0.5%	33.3%	$ 1,825
Healthcare/Medicaid/Medicare	5.4	0.8%	19.4%	$ 480
Home improvement	138.3	1.4%	70.1%	$ 1,800
Identity theft	10.7	1.0%	33.8%	$ 400
Investment/cryptocurrency	561.6	1.8%	80.1%	$ 5,000
Moving	6.1	0.2%	74.1%	$ 623
Online purchase	152.8	30.3%	87.5%	$ 75
Phishing/social engineering	56.7	16.4%	10.6%	$ 423
Rental	12.0	0.5%	64.1%	$ 500
Retail business imposter	8.5	1.6%	40.9%	$ 175
Romance/friendship	196.9	0.7%	64.5%	$ 6,099
Sweepstakes/lottery/prizes	10.7	2.6%	18.0%	$ 300
Tax collection	3.4	0.2%	12.2%	NA
Tech support	19.2	1.4%	31.0%	$ 561
Travel/vacation/timeshare	33.2	2.0%	38.0%	$ 573
Utility	5.8	0.7%	25.8%	$ 435
Other	52.6	6.9%	41.5%	$ 240

NA: This scam type did not have enough reports with a dollar loss to include a median dollar loss.

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

	RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN $ LOSS
1	Investment/ cryptocurrency	Online purchase	Online purchase	Romance/friendship
2	Employment	Phishing/social engineering	Counterfeit product	Investment/ cryptocurrency
3	Romance/friendship	Employment	Investment/ cryptocurrency	Government grant
4	Online purchase	Debt collection	Moving	Home improvement
5	Home improvement	Sweepstakes/ lottery/ prizes	Home improvement	Employment
6	Phishing/social engineering	Counterfeit product	Romance/friendship	Family/friend emergency
7	Advance fee loan	Government agency imposter	Rental	Fake check/ money order
8	Travel/vacation/ timeshare	Travel/vacation/ timeshare	Credit repair/ debt relief	Advance Fee Loan
9	Government grant	Investment/ cryptocurrency	Retail business imposter	Credit repair/ debt relief
10	Tech support	Advance fee loan	Travel/vacation/ timeshare	Moving

INSTITUTE for MARKETPLACE TRUST[SM]

BBB Institute for Marketplace Trust[SM]
4250 North Fairfax Drive, Suite 600
Arlington VA 22203

Institute@IABBB.org

BBBMarketplaceTrust.org/RiskReport