2025 BBB Scam Tracker℠

Risk Report

BETTER BUSINESS BUREAU

2025 BBB Scam Tracker℠

Risk Report

BETTER BUSINESS BUREAU

Introduction

Scams hurt everyone. They cost people money, create stress, and make it harder to trust businesses and online interactions. A safe and trustworthy marketplace depends on people having the information they need to spot scams and honest businesses taking action to protect their customers.

The BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the International Association of Better Business Bureaus®, is proud to share the *2025 BBB Scam Tracker Risk Report*. This annual report looks at scam reports submitted by consumers and businesses to BBB Scam Tracker℠ (BBB.org/ScamTracker) during 2025. By analyzing this data, we can better understand how scammers operate, who they target, which scams cause the most harm, and what factors may make someone more vulnerable. Highlights of the report are provided in the infographic on page 7.

BBB Institute works with trusted partners to turn these insights into practical education and tools that help people protect themselves and their loved ones. Using the network of Better Business Bureaus across the United States and Canada, we share timely scam alerts and educational resources both online and in local communities so people can stay informed. This report is just one example of how we take feedback from the public and turn it into resources that can empower people to protect themselves.

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. BBB reviews and posts these reports, allowing the public to search the website and determine whether they are being targeted.

According to a survey of people who filed BBB Scam Tracker reports in 2025,[1] 31.2% of visitors said they visited the BBB Scam Tracker website to find out if they were experiencing what could be a scam, and 41.3% of those said BBB Scam Tracker helped them avoid losing money when targeted by a scam. With more than 3.2 million people visiting the platform in 2025,[2] we estimate BBB Scam Tracker helped people avoid losing more than $38 million in 2025 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.

1 Web-intercept survey with 2,621 unique respondents who visited BBB Scam Tracker in January 2025. Respondents could choose multiple reasons for visiting BBB Scam Tracker.

2 Adobe Analytics.

We estimate BBB Scam Tracker helped people avoid losing almost $39 million in 2025 alone.

FIGURE 1
2025 BBB Scam Tracker impact

3,251,807

Unique visitors to BBB Scam Tracker

31.2%

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

41.3%

Of those visitors said BBB Scam Tracker helped them avoid losing money

$93

Overall median reported U.S. dollar loss in 2025

$38,968,380

Estimated dollar amount people **avoided losing** thanks to BBB Scam Tracker

Snapshot of 2025

The data provided via BBB Scam Tracker reports help us understand how scams are being perpetrated in the marketplace. In 2025, BBB Scam Tracker published more than 146,000 reported scams. We classified scam reports submitted by individuals and businesses across the United States and Canada into 32 scam types and an "other" category that represented 6.1% 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 to report. See Appendix B and Appendix C for detailed data by scam type.

Findings in this year's report highlight the complexity of today's scams. Scammers continue to evolve their tactics, using new technologies and currencies, multiple contact and payment methods, and an ever-changing online world to steal people's money and personal information. For some scam types, fraudsters spend a significant amount of time building relationships that result in high financial losses and an emotional toll that can be life-changing for victims. See page 44 for more information on the non-financial impact of scams.

Findings in this year's report highlight the complexity of today's scam tactics.

Reported susceptibility and median dollar loss decrease

In 2025, susceptibility (the percentage of people who reported losing money when exposed[3] to a scam) decreased from 44.4% in 2024 to 39.8% in 2025 (Figure 2). Reported median dollar loss decreased from $130 in 2024 to $93 in 2025.

Riskiest scams

The top two riskiest scams remained the same (investment/cryptocurrency scams at No. 1 and employment scams at No. 2). Online purchase scams rose to No. 3 riskiest, dropping romance/friendship scams to No. 4 riskiest. More information about the list of riskiest scams can be found on page 11.

[3] Throughout this report when we reference exposure, note that 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.

How scammers engaged their targets

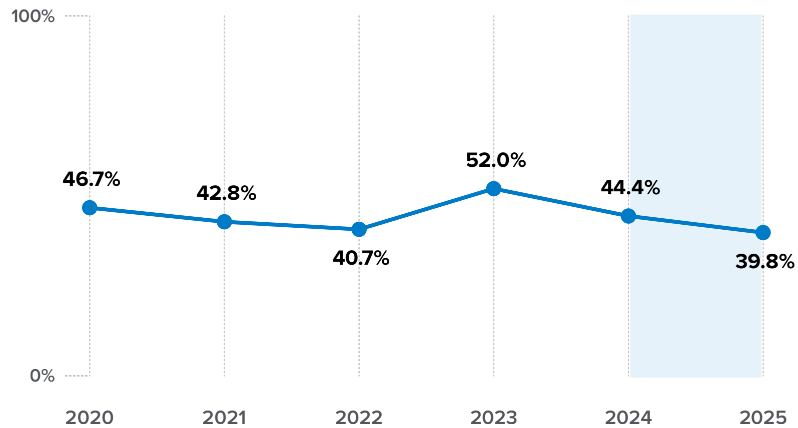
The most reported contact methods scammers used to engage people in 2025 included phone call, email, and text message. Credit cards remained the top reported payment method, followed by bank account debit and online payment system (digital payment app).

FIGURE 2

Snapshot of 2025 compared with previous years

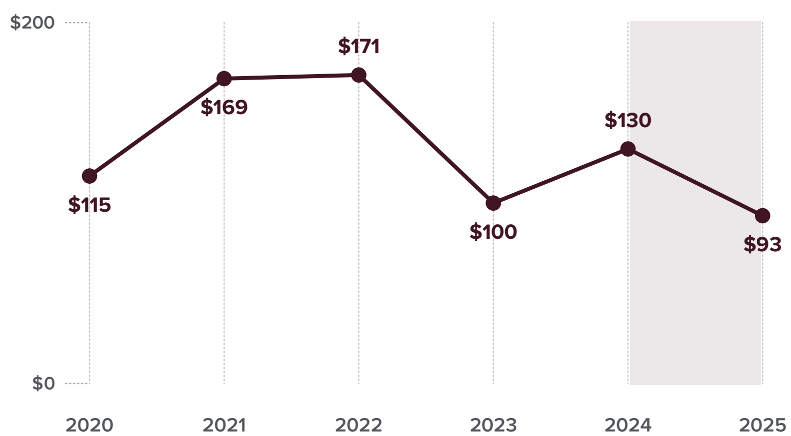
SUSCEPTIBILITY
Percentage of reports that include a dollar loss

10.4%
DECREASE
from 2024



MONETARY LOSS*
Median reported dollar loss

28.5%
DECREASE
from 2024



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

Snapshot of 2025

2025 *Risk Report* Highlights

Likelihood of Loss
(Susceptibility)

39.8%

DECREASED 10.4% from 2024 (44.4%)

Median Dollar Loss

$93

DECREASED 28.5% from 2024 ($130)

Top 3 Riskiest Scams
reported by consumers[5]

1. **Investment/ cryptocurrency scams**
2. **Employment scams**
3. **Online purchase scams**

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

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

KEY HIGHLIGHTS

Investment/cryptocurrency scams remained the No. 1 riskiest scam type in 2025, with the highest median dollar loss reported of all scam types ($5,000); 77.4% of reports included a monetary loss.

Employment scams remained the No. 2 riskiest scam type, with a median dollar loss of $1,000; this type of scam made up more than 15% of all reported scam types. See page 16 for more information.

Online purchase scams rose from No. 4 in 2024 to No. 3 riskiest in 2025. This scam type made up more than 28% of all scams reported to BBB Scam Tracker, with 89.3% reporting a dollar loss.

Romance/friendship scams, at No. 4 riskiest, had the second-highest median dollar loss ($4,500) of all scam types.

People ages 25–34 and 65+ reported the highest median dollar loss ($100). People ages 65+ submitted a higher percentage of reports with a monetary loss (susceptibility) than other age groups; this group reported the lowest susceptibility in 2024.

Social media was the contact method with the highest percentage of reports with a dollar loss. Text message scams rose from 9.8% of all reported scams in 2024 to 14.9% in 2025.

PayPal was the organization most often impersonated by scammers in 2025, according to reports submitted to BBB Scam Tracker.

2025 *Risk Report* Highlights

SURVEY RESEARCH HIGHLIGHTS[6]

28.7%

reported that their **mental health was impacted by the scam incident.** The No. 1 emotion they reported was anger (65.1%), followed by loss of trust (55.8%) and anxiety/stress/trauma (54.4%). See page 45.

TOP PLATFORMS

on which survey respondents reported engaging with the scammers were **Facebook (56.1%), Instagram (17.5%), and TikTok (11.3%).** See page 27.

40%

said they **realized they were experiencing a scam within 24 hours.** Those who engaged with the scammer for more than one day were more likely to report losing money. See page 41.

FAKE ADS ON SOCIAL MEDIA

Respondents reported being **less confident in reporting fake ads on social media** than they did reporting scams they experienced via phone or email. See page 42.

14.7%

of survey respondents **reported losing money at least three times,** up from 12.4% in 2024. Notably, 4.6% reported losing money five or more times, up from 3.8% in 2024. See page 43.

[6] A survey was distributed to those who submitted a scam to BBB Scam Tracker in 2025; 2,820 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 based on three factors: exposure, susceptibility, and monetary loss. This unique formula makes up the BBB Risk Index (Figure 3). 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 typically reach fewer people, but those exposed individuals are often more likely to lose money and to lose higher amounts of money.

FIGURE 3
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

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.

10 riskiest scams reported by consumers in 2025

Each year, BBB Institute publishes its list of the 10 riskiest scam types (Table 1), which we calculate using the BBB Risk Index (Figure 3) and reports submitted to BBB Scam Tracker. In 2025, investment/cryptocurrency scams remained the No. 1 riskiest scam type, with 77.4% of those targeted reporting a monetary loss. The median dollar loss ($5,000) was significantly higher than the median dollar loss reported for scams overall ($93). Employment scams remained the No. 2 riskiest scam, making up 15.8% of all scams published on BBB Scam Tracker, up from 14.4% in 2024.

Investment/ cryptocurrency scams remained the No. 1 riskiest scam type, followed by employment scams.

Online purchase scams became the No. 3 riskiest scam type in 2025, comprising the largest volume of any scam type (28.4% of all published scams). Romance/friendship scams dropped to No. 4 riskiest. New to the top 10 riskiest list this year are counterfeit product, debt collection, and sweepstakes, lottery, prize scams. The percentage of people who reported losing money to counterfeit product scams increased from 80.7% to 90.5%; exposure rose from 2.1% of all scams published on BBB Scam Tracker in 2024 to 3.1% in 2025. Phishing/ social engineering scams remained No. 6 on the list. This scam type comprised 18.2% of all reports submitted in 2025.

Scam types with high susceptibility

The scam types with the highest percentage of reports with a dollar loss included counterfeit product (90.5%), online purchase (89.3%), investment/cryptocurrency (77.4%), and moving (76.1%). A full breakout of the scam types with the highest susceptibility can be found on page 57.

Scam types with high median dollar loss

The scam types with the highest median dollar loss included investment/cryptocurrency ($5,000), romance/friendship ($4,500), fake check/money order ($1,474), and home improvement ($1,405). A full breakout of scam types with the highest median dollar loss can be found on page 57.

10 riskiest scams reported by consumers in 2025

TABLE 1

10 riskiest consumer scams in 2025

RANK		SCAM TYPE	BBB RISK INDEX	EXPOSURE		SUSCEPTIBILITY		MEDIAN $ LOSS	
2025	2024			2025	2024	2025	2024	2025	2024
1	1	Investment/ cryptocurrency	564.7	1.4%	1.8%	77.4%	80.1%	$5,000	$5,000
2	2	Employment	227.4	15.8%	14.4%	13.3%	17.2%	$1,000	$1,500
3	4	Online purchase	185.4	28.4%	30.3%	89.3%	87.5%	$68	$75
4	3	Romance/ friendship	123.5	0.4%	0.7%	71.7%	64.5%	$4,500	$6,099
5	5	Home improvement	96.2	0.9%	1.4%	69.1%	70.1%	$1,405	$1,800
6	6	Phishing/social engineering	41.8	18.2%	16.4%	6.6%	10.6%	$325	$423
7	8	Travel/ vacation/ timeshare	35.3	1.0%	2.0%	55.8%	38.0%	$580	$573
8 *(tied)*	7	Advance fee loan	23.9	4.1%	1.7%	6.7%	30.1%	$800	$1,000
8 *(tied)*	14	Counterfeit product	23.9	3.1%	2.1%	90.5%	80.7%	$80	$84
9	12	Debt collection	11.7	4.5%	5.4%	4.8%	5.8%	$500	$500
10	16	Sweepstakes/ lottery/prizes	10.3	1.6%	2.6%	19.8%	18.0%	$300	$300

Scam types ranked by highest median loss (90th percentile)

Although overall median dollar loss offers a broad view of a scam's impact, it can mask the severe financial harm experienced by individual victims. To better illustrate this risk, the scam types in Table 2 are ranked based on losses in the top 10 percent of reported cases, showing the median loss among the highest-loss incidents for each category.

TABLE 2

Highest-loss incidents

RANK	SCAM TYPE	MEDIAN $ LOSS
1	Investment/ cryptocurrency	$82,100
2	Romance/friendship	$70,000
3	Home improvement	$14,050
4	Fake check/money order	$13,795
5	Government grant	$11,911

2025 riskiest consumer scams

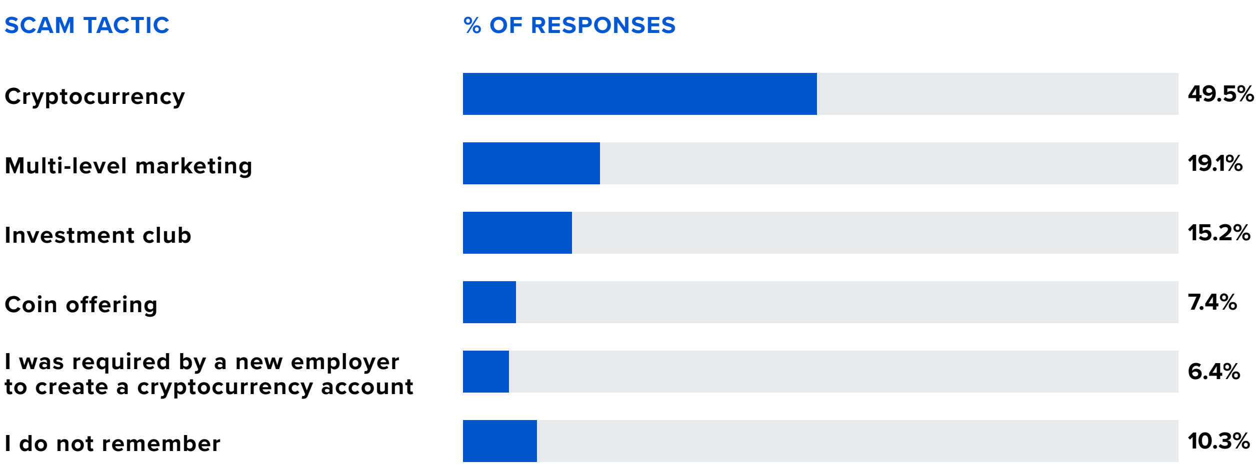
Investment/cryptocurrency scams

Investment scams are perpetrated in a variety of ways, but all promise large returns with little or no risk. Almost 50% of survey respondents who reported being targeted by an investment scam said the incident involved cryptocurrency (Figure 4).

More than 26% of survey respondents said they were introduced to the investment opportunity by an advertisement or social media post; 19% said they were introduced by an online contact.

FIGURE 4

Did the investment scam involve any of the following?



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

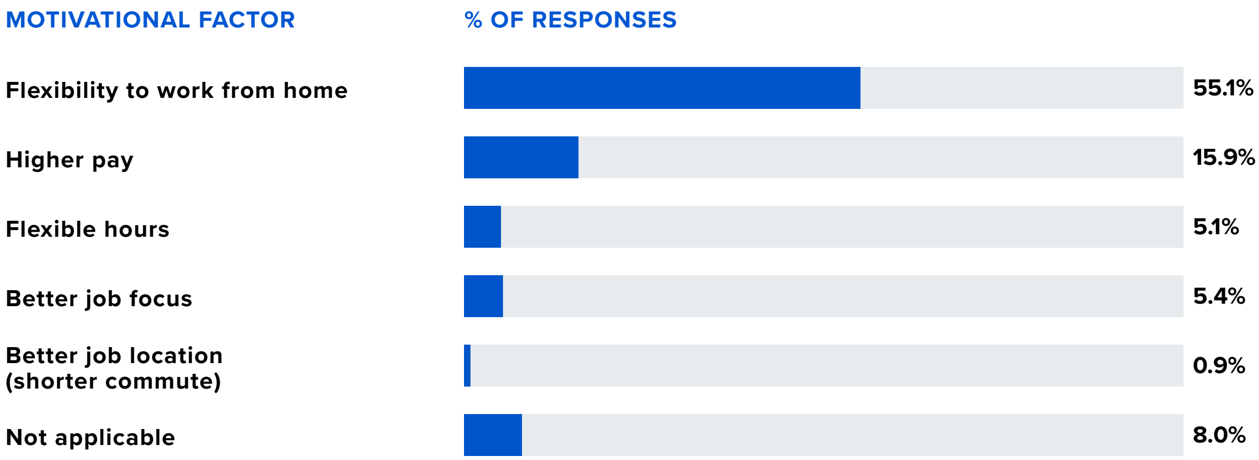
Employment scams

The tactics used to perpetrate employment scams have shifted over the past few years (see page 16). Flexibility to work from home was, by far, the most reported motivational factor for engaging with the scam (Figure 5).

Survey respondents who said they were content with their job but were searching for more income or were open to new opportunities were more likely to report losing money than active job seekers (Figure 6).

FIGURE 5

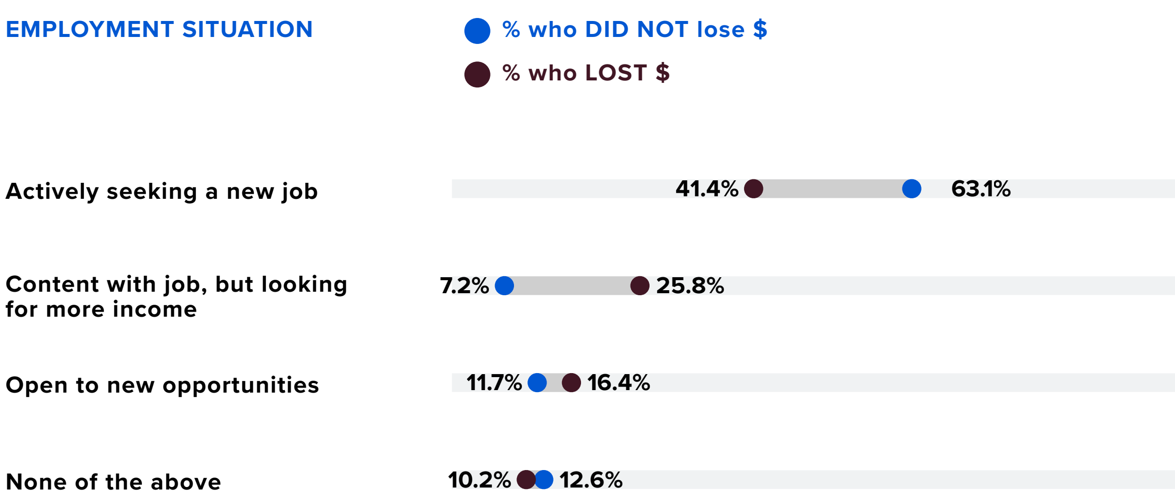
What was the biggest motivational factor that made you engage with the job scam/recruiter?



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

FIGURE 6

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 is not included.

Romance/friendship scams

About 46.3% of survey respondents reporting a romance/friendship scam said they were encouraged by the scammer to deposit money into a cryptocurrency account. Not all survey respondents ended the engagement immediately once they recognized the scam (Figure 7). Although friendship/romance scams can involve different types of relationships, 57.4% reported that the scam incident was romantic in nature (Figure 8).

FIGURE 7

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

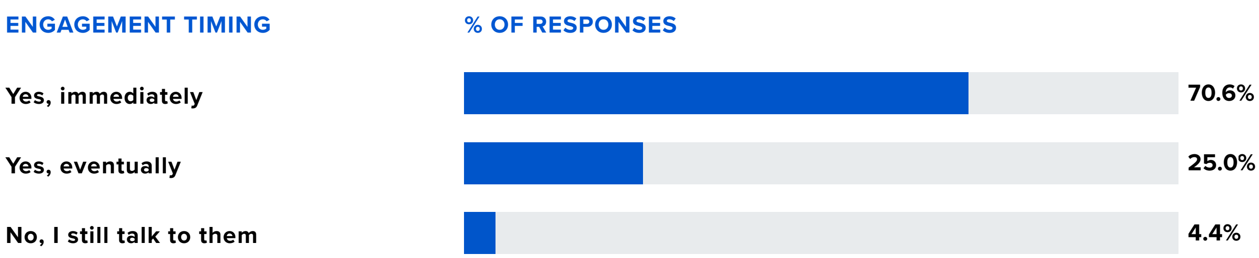
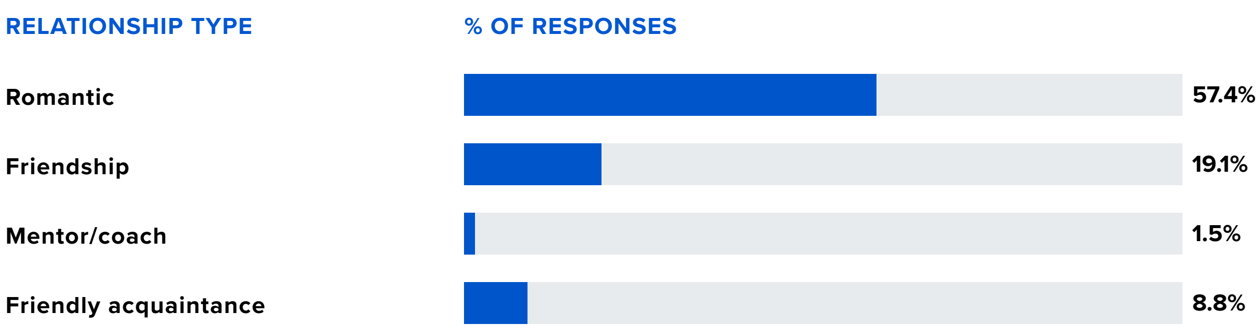


FIGURE 8

Please choose the best description of the relationship:



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

Online purchase and counterfeit product scams

Online purchase and counterfeit products both ranked in the top 10 list of riskiest scams. Consumers paid for products they never received. In other cases, they received counterfeit items of inferior quality. The most mentioned product categories used for online purchase or counterfeit scams were apparel, pets, and cars/machines (Table 3).

Phishing/social engineering scams

Reports of phishing/social engineering scams increased from 16.4% of all scams published on BBB Scam Tracker in 2024 to 18.2% in 2025. Survey respondents who reported a phishing/social engineering scam engaged in a variety of ways, including phone calls from scammers pretending to be trustworthy organizations (38.4%), impersonation email and/or text messages (33.9%), and malicious links/attachments (26.1%). Survey respondents reported scammers stole a wide range of personally identifiable information (Figure 9).

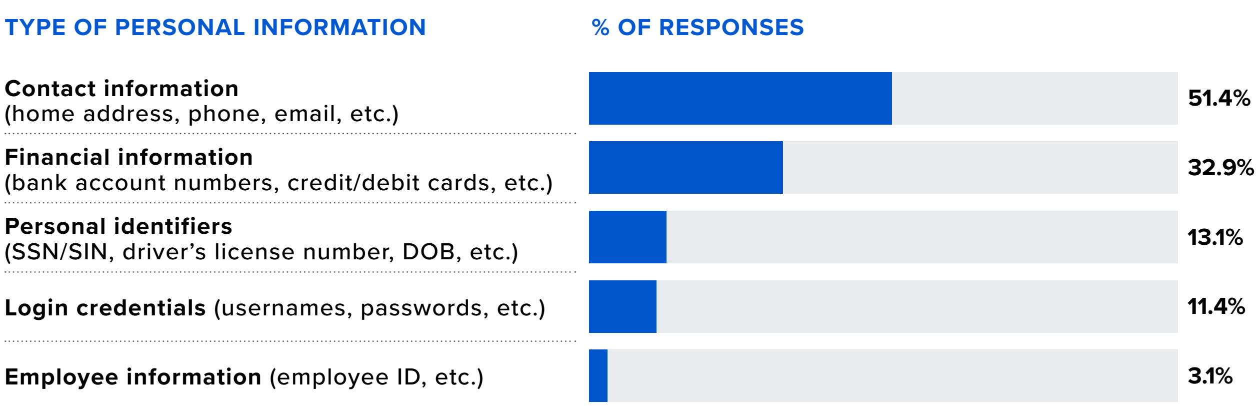
TABLE 3

Most mentioned products in online purchase/counterfeit scam reports

PRODUCT CATEGORY	TOTAL MENTIONS
Apparel	6,426
Pets	3,145
Cars/machines	3,049
Footwear	2,439
Furniture/appliances	2,121
Medical/nutrition	1,444
Toys and collectibles	1,376
Jewelry	1,276
Cosmetics	1,117
Digital devices	977
Luggage/handbags	583

FIGURE 9

What personal information did the scammer collect during the phishing/social engineering incident?



The percentages do not add up to 100% because respondents were allowed to choose more than one answer.

Employment scams rise, tactics shift

Employment scams—ranked No. 2 riskiest since 2022—lure victims with seemingly legitimate, too-good-to-be-true job opportunities designed to steal money or personal information. These scams were especially prevalent among younger adults, ranking as the No. 1 riskiest scam type in 2025 for individuals ages 18–34. Reports to BBB Scam Tracker show that employment scams increased from 14.4% of all published reports in 2024 to 15.8% in 2025.

New tactics on the rise

In recent years, a common employment scam involved an overpayment scheme in which victims are instructed to deposit a check for training or home office equipment and then to quickly transfer most of the funds elsewhere, only to later discover the check was fraudulent. This tactic remains in use, and it now accounts for 20.4% of employment scams, according to survey findings. Another popular tactic, making up 32.4% of reported cases, involves fake job applications designed to steal personal information.

A newer and increasingly common job scam tactic targets individuals hired for online marketing roles, such as posting product reviews.

Victims are initially paid through an online account—sometimes using cryptocurrency—but are later told they must deposit additional funds or pay fees or taxes to access their earnings. In some cases, victims are placed in group chats with supposed coworkers who normalize these requests, though they are often part of the scam. This tactic accounted for 25.5% of employment scams reported through survey research.

Contact and payment method

Text messages (51.4%) and email (25.7%) were the most common methods scammers used to perpetrate employment scams. Cryptocurrency was the most frequently reported payment method for employment scams, cited in 35.1% of cases.

Employment scams rise, tactics shift

The following scam report was submitted to BBB scam Tracker:

The scammer offered a job that asked me to do product reviews for money. In return, I would receive a daily amount that I could withdraw after completing 40 separate product reviews (40 reviews equals one set; after you complete 2 sets, you have done your daily job). Each day, you could withdraw money after your job was done.

I only completed jobs for 5 days before I knew I was being scammed. Each day, there was a chance you would receive an order that made you pay money in order to complete the review for that product. Some days it was $60, and some were even up to $300. The only way for you to get your daily pay was to place money in your account so you could continue making reviews on products. If you did not complete your 2 sets of reviews, you could not get paid.

I was told I had to pay $3,000 to complete a job task, otherwise I would not get paid. My "mentor" kept advising me to send the funds to finish the job. I was also in a group chat, and once I started calling out my suspicions, no one batted an eye. No one was concerned about their money being scammed from them, as if they were all in on the activity. I deposited over $1,800 in 5 days, and all that money is gone.[7]

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

I was told I had to pay $3,000 to complete a job task, otherwise I would not get paid.

Employment scams rise, tactics shift

Prevention Tips

Be wary of offers that seem too good to be true. Scammers offer work-from-home opportunities, good pay, and other goodies to attract victims.

Legitimate job offers do not come with up-front fees. If you are paying for the promise of a job, or contributing your own funds in order to get paid, it's probably a scam.

Always do background research on the job offer (find the job listing on the company's website).

Be wary of work-from-home offers, especially shipping/warehouse opportunities, secret shopper positions, and online marketing jobs in which you'll be paid via their account.

Beware of offers made too quickly or without an interview.

Be wary if the "employer" asks you to deposit a check and transfer funds to another account for training or equipment or for any other reason. Fake check scams are a common tactic used for job scams.

Be wary of vague job descriptions. To reach as many people as possible, scammers list job requirements that are broad enough to enable anyone to qualify

Scams perpetrated via text message continue to rise

Our phones are always within reach—for work, personal matters, and everything in between. That constant connection is exactly why text message scams are so concerning. These messages often arrive without warning, tempting us with unbelievable offers or pressuring us to act immediately to avoid a supposed problem. When scammers trigger urgency or fear, people may respond without stopping to think, putting their money or personal information at risk.

Data from BBB Scam Tracker shows that text message scams rose from 9.8% of all published scams in 2024 to 14.9% in 2025.

The following scam report was submitted to BBB Scam Tracker:

> *She sent a text message to a supposed wrong number then introduced herself as Reine. She then convinced me to talk to her via WhatsApp. It ended up leading to a romantic relationship where she convinced me to use a crypto trading platform called mdexus.net.*
>
> *I ended up emptying my IRA and taking a loan out to invest in so-called guaranteed profits. She wanted me to invest more but I couldn't. I'm now trying to withdraw some money, but the website says it needs me to pay more tax and that it can't deduct it from the amount. This is a catfish scam [intended] to steal money from lonely men.*[8]

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

I ended up emptying my IRA and taking a loan out to invest in so-called guaranteed profits.

Scams perpetrated via text message continue to rise

Prevention Tips

Be skeptical of strangers

Ignore unsolicited communications and messages from random numbers. Avoid developing online "relationships" with promises of financial gain.

Verify investments thoroughly

For any investment opportunity, do your research and verify the person and the opportunity:

- **Check licensing:** Confirm any platform's registration with regulatory bodies (SEC, FINRA) using tools like FINRA BrokerCheck.
- **Research platforms:** Look up websites/apps with domain checkers (check age) and scan reviews for legitimacy.
- **Consult experts:** Talk to a trusted, independent financial advisor before investing.

Don't trust unsolicited messages

If an out-of-the-blue offer sounds too good to be true, it probably is. If you receive an unexpected text message asking you to respond, look up the organization's contact information on the official website.

Watch out for suspicious links

Many scam text messages contain a link. Scammers hope their message will cause you to feel so scared or excited you'll click the link without thinking. Some of these links could download malware onto your device.

Look up phone numbers before you call

Scammers may prompt you to call a number, claiming you need to resolve some kind of issue or register to receive a prize. Never call the number they provide you.

Don't share personal information

Never share your PIN, password, social security or social insurance number, or other personal details with somebody on an unsolicited call, text, or email.

If you spot a scam text, don't reply

Some scammers ask you to text "STOP" or "NO" so you won't receive future texts. In reality, your reply tells them they have a real, active phone number, and this could open you up to future attacks. If a text message seems suspicious, don't reply. Block the number and erase the message.

Demographics

Self-reported data provided through BBB Scam Tracker combined with survey research help us better understand how scams are impacting different demographics. This information enables BBB to target outreach and educational strategies aimed at empowering consumers and businesses to identify and avoid scams.

Age

This year, people ages 25–34 and 65+ reported the highest median dollar loss ($100), followed by people ages 18–24 ($98) (Figure 10). People ages 65+ submitted a higher percentage of reports with a monetary loss (susceptibility) than other age groups; this group reported the lowest susceptibility in 2024.

Table 4 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+ submitted a higher percentage of reports with a monetary loss than other age groups.

FIGURE 10

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

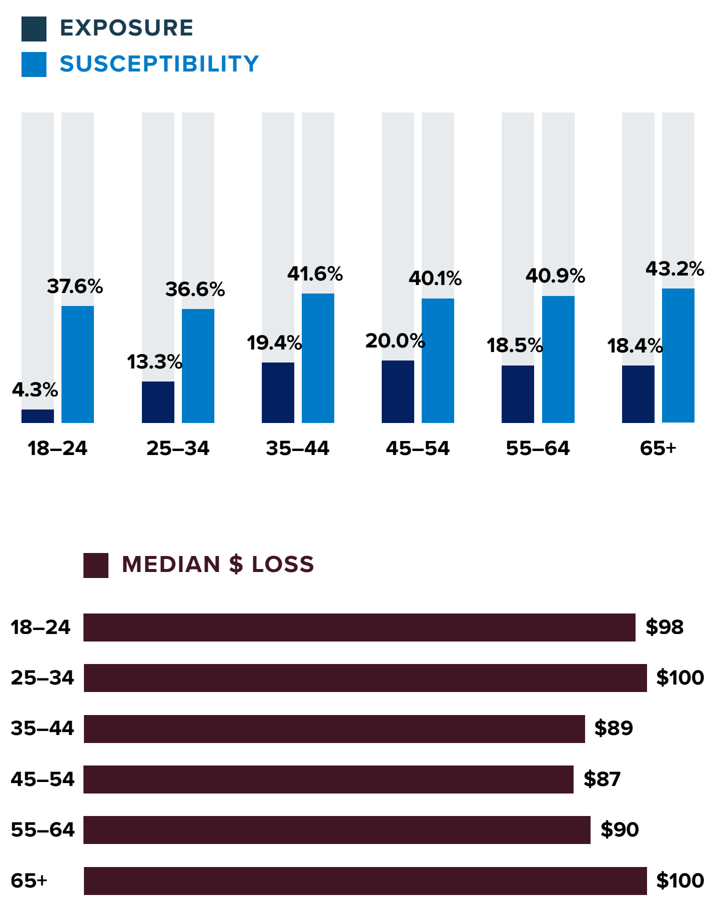


TABLE 4

Three riskiest scam types by age

AGE	NO. 1 RISKIEST SCAM	NO. 2 RISKIEST SCAM	NO. 3 RISKIEST SCAM
18–24	Employment	Investment/cryptocurrency	Online purchase
25–34	Employment	Investment/cryptocurrency	Online purchase
35–44	Investment/cryptocurrency	Employment	Online purchase
45–54	Investment/cryptocurrency	Employment	Online purchase
55–64	Investment/cryptocurrency	Employment	Online purchase
65+	Investment/cryptocurrency	Romance/friendship	Online purchase

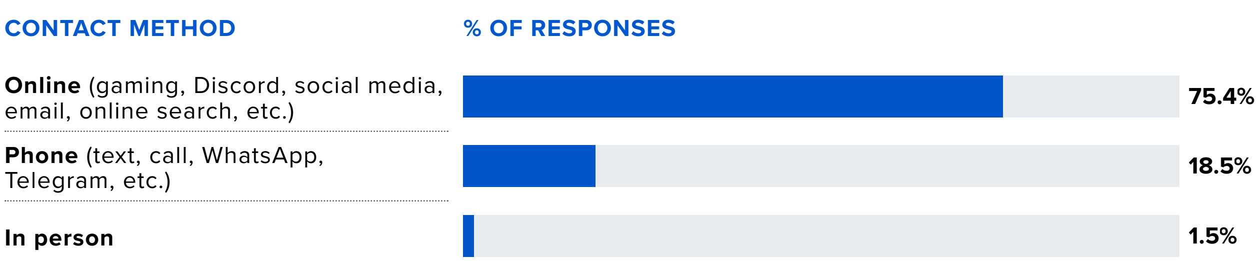
Scams targeting youth

BBB Scam Tracker does not collect information from people younger than age 18. Of the 19.9% of survey respondents who reported having children younger than 18, 11.4% said their children were targeted by scams. Respondents reported that their children were contacted via gaming platforms, social media, text message, phone call, and more (Figure 11).

Parents reported their children were primarily engaged with scammers on gaming platforms (47.9%) and social media (27.1%). They reported that their children, when targeted by phone, were targeted via text messages (58.3%), phone calls (25.0%), and messaging apps (8.3%).

FIGURE 11

Where was your child first targeted/contacted by the scammer?



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

Gender

Females submitted 62% of scam reports to BBB Scam Tracker in 2025 (Figure 12). Females reported being more susceptible to losing money when exposed to a scam (41.3%) compared to males (37.4%) and nonbinary people (27.7%).

The reported median dollar loss was lower for females ($82) than for males ($135) and nonbinary people ($100). Females and males reported the same top three riskiest scam types (Table 5). Employment scams were No. 1 riskiest for nonbinary people.

FIGURE 12

Exposure, susceptibility and median dollar loss by gender (all scam types)

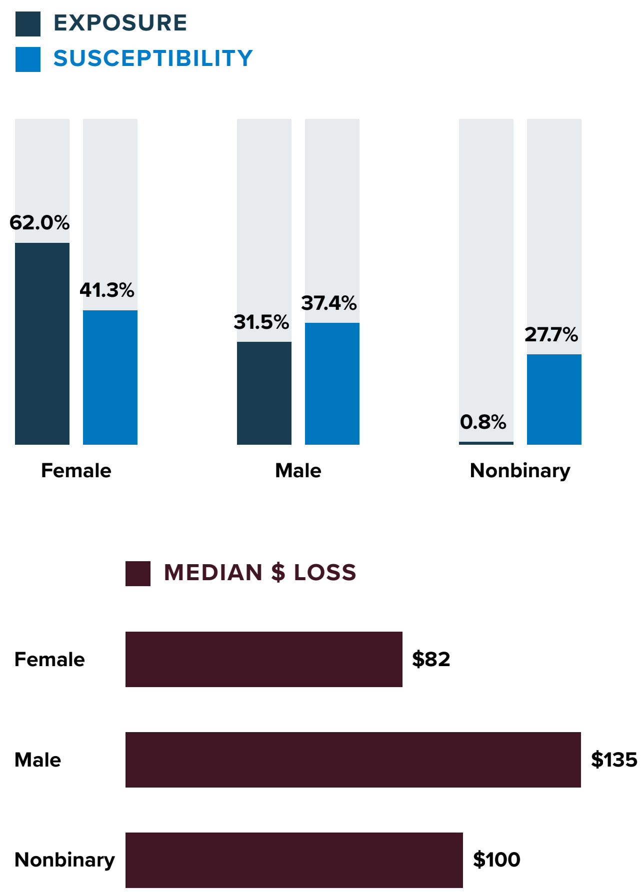


TABLE 5

Riskiest scam types by gender

GENDER	NO. 1 RISKIEST SCAM	NO. 2 RISKIEST SCAM	NO. 3 RISKIEST SCAM
Female	Investment/cryptocurrency	Employment	Online purchase
Male	Investment/cryptocurrency	Employment	Online purchase
Nonbinary	Employment	Debt collection	Online purchase

Contact methods

The most reported contact methods scammers used to engage people in 2025 included phone call, email, and text message. The contact methods with the highest percentage of reports with a monetary loss (susceptibility) were social media, website, and in person (Figure 13).

More than 87% reported losing money when they engaged with the scammer via social media, up from 82.5% in 2024 (Figure 13). Susceptibility also rose for contact by website, up from 79.7% in 2024 to 83.0% in 2025. Those who reported losing money when contacted via internet messaging has continued to rise, from 59.9% in 2023 and 68.9% in 2024 to 72.9% in 2025.

Rise in text message/phone scams

Reported text message scams rose from 9.8% of all scams published on BBB Scam Tracker in 2024 to 14.9% in 2025. Scams perpetrated via phone also rose from 23.8% of all reported scams in 2024 to 26.3% in 2025.

Online scams

Scams perpetrated online are more likely to result in a monetary loss than those perpetrated in person or via phone (Figure 14).

Reported text message scams rose from 9.8% of all scams published on BBB Scam Tracker in 2024 to 14.9% in 2025.

Older people were more likely to report losing money when targeted by online classifieds and internet messaging (Figure 15). Younger people were more likely to report losing money by engaging via text message or in person.

Shifting contact methods

According to our survey research, 16.4% of respondents reported that the scammer asked them to switch communication channels during the incident. Scammers often urge victims to move away from platforms that might detect suspicious activity or issue warnings, steering the interaction instead to channels where the scam can continue with a lower risk of interruption or intervention.

Social media scams

Survey respondents primarily engaged with scammers on social media via advertisements (39.6%), an effort to purchase from somebody (32.2%), and via direct message (22.2%) (Figure 16). Again this year, Facebook was the platform most reported as the place people engaged with a scammer (Figure 17).

Contact methods

FIGURE 13

Contact method with a monetary loss

CONTACT METHOD	% OF ALL REPORTS	SUSCEPTIBILITY	MEDIAN $ LOSS
Phone call	26.3%	12.6%	$600
Email	24.2%	29.3%	$82
Text message	14.9%	9.5%	$700
Website	13.9%	83.0%	$84
Social media (e.g., Facebook)	13.5%	87.8%	$64
Internet messaging (e.g., WhatsApp)	2.0%	72.9%	$850
In person	1.2%	75.1%	$1,300
Online classifieds (e.g., Craigslist)	0.8%	61.3%	$99
Fax	0.2%	4.8%	$200
Other	2.4%	57.7%	$99

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

FIGURE 14

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

ONLINE

54.3%
of all scams reported

81.5%
of all scams reported with a $ loss

PHONE

41.4%
of all scams reported

11.9%
of all scams reported with a $ loss

IN PERSON

1.2%
of all scams reported

2.2%
of all scams reported with a $ loss

Percentages of all scams and scams with a monetary loss do not add up to 100% because the "other" category is not included. Means of contact includes online (website, social media, email, internet messaging, and online classifieds), phone (phone, text, fax), and in person.

FIGURE 15

Contact method by age (reports with a monetary loss)

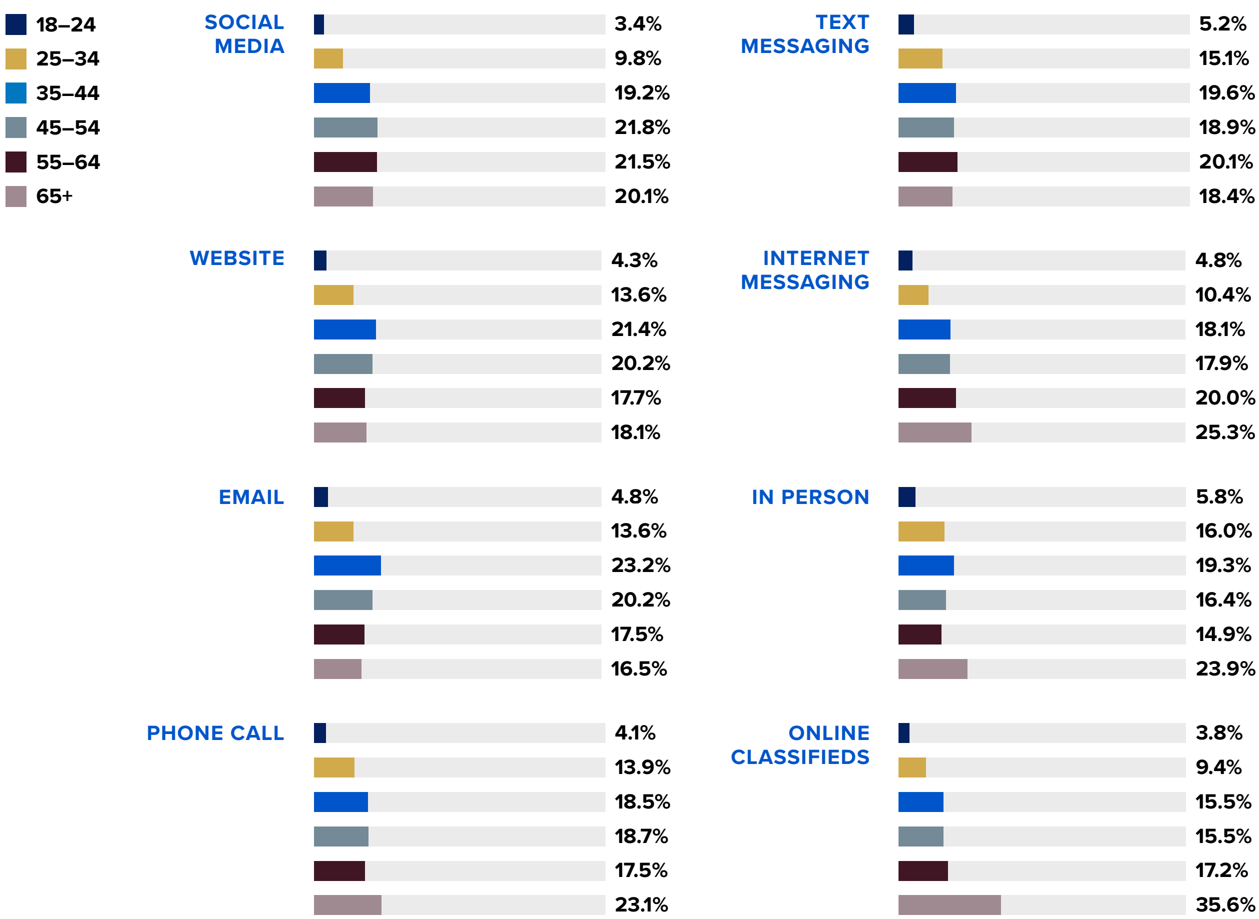


TABLE 6

Most reported scam types by contact method

CONTACT METHOD	NO. 1 MOST REPORTED	NO. 2 MOST REPORTED	NO. 3 MOST REPORTED
Website	Online purchase	Counterfeit product	Employment
Social media	Online purchase	Counterfeit product	Employment
Internet messaging	Employment	Online purchase	Investment/ cryptocurrency
Online classifieds	Online purchase	Employment	Counterfeit product
Email	Phishing/ social engineering	Online purchase	Employment
Text message	Employment	Phishing/ social engineering	Advance fee loan
In person	Home improvement	Retail business imposter	Counterfeit product
Phone call	Phishing/ social engineering	Debt collection	Advance fee loan

FIGURE 16

How did you engage with the scammer on social media?

ENGAGEMENT TACTIC	% OF RESPONSES
I responded to a social media ad	39.6%
I tried to buy something from them (peer-to-peer transaction)	32.2%
They sent me a direct message	22.2%
I responded to a social media post	15.0%
They sent me a friend request	5.1%
They pretended to be a celebrity	4.6%
They commented on or reacted to my post	3.8%
They added me to a chat group	3.5%
They pretended to be somebody I know	3.2%
We met in a social media group	1.3%
I do not remember	2.9%

The responses do not add up to 100% because respondents were allowed to choose more than one answer.

FIGURE 17

Top reported online platforms

ONLINE PLATFORM	% OF RESPONSES
Facebook	56.1%
Instagram	17.5%
TikTok	11.3%
Facebook Marketplace	10.4%
WhatsApp	8.2%
Telegram	5.7%
LinkedIn	4.1%
Indeed	2.8%
YouTube	2.5%
X (formerly Twitter)	2.3%

The responses do not add up to 100% because respondents were allowed to choose more than one answer.

Payment methods

Credit cards remained the top reported payment method (Figure 18), followed by bank account debit and online payment system (digital payment app). Reports of people paying with credit cards rose from 39.4% in 2024 to 44.7% in 2025. Payment methods with the highest median dollar loss were wire transfer, cryptocurrency, and check.

When monetary loss is broken out by age and payment method (Figure 19), older people reported a higher percentage of instances in which they paid via prepaid/gift card and check. Younger people submitted a higher percentage of reports that they paid via cash, money order, and bank account debit. People ages 35–54 were more likely to pay with cryptocurrency than other age groups.

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 7). Employment scams were the most reported scam type in which reporters said they paid via cryptocurrency in 2025; investment/cryptocurrency scams dropped to the second most reported scam type paying with cryptocurrency.

Scammers sometimes request people pay using multiple payment methods; about 15.8% of survey respondents reported using multiple payment methods during the scam incident.

Online purchase scams were the most reported scam type for several payment methods.

Payment methods

FIGURE 18

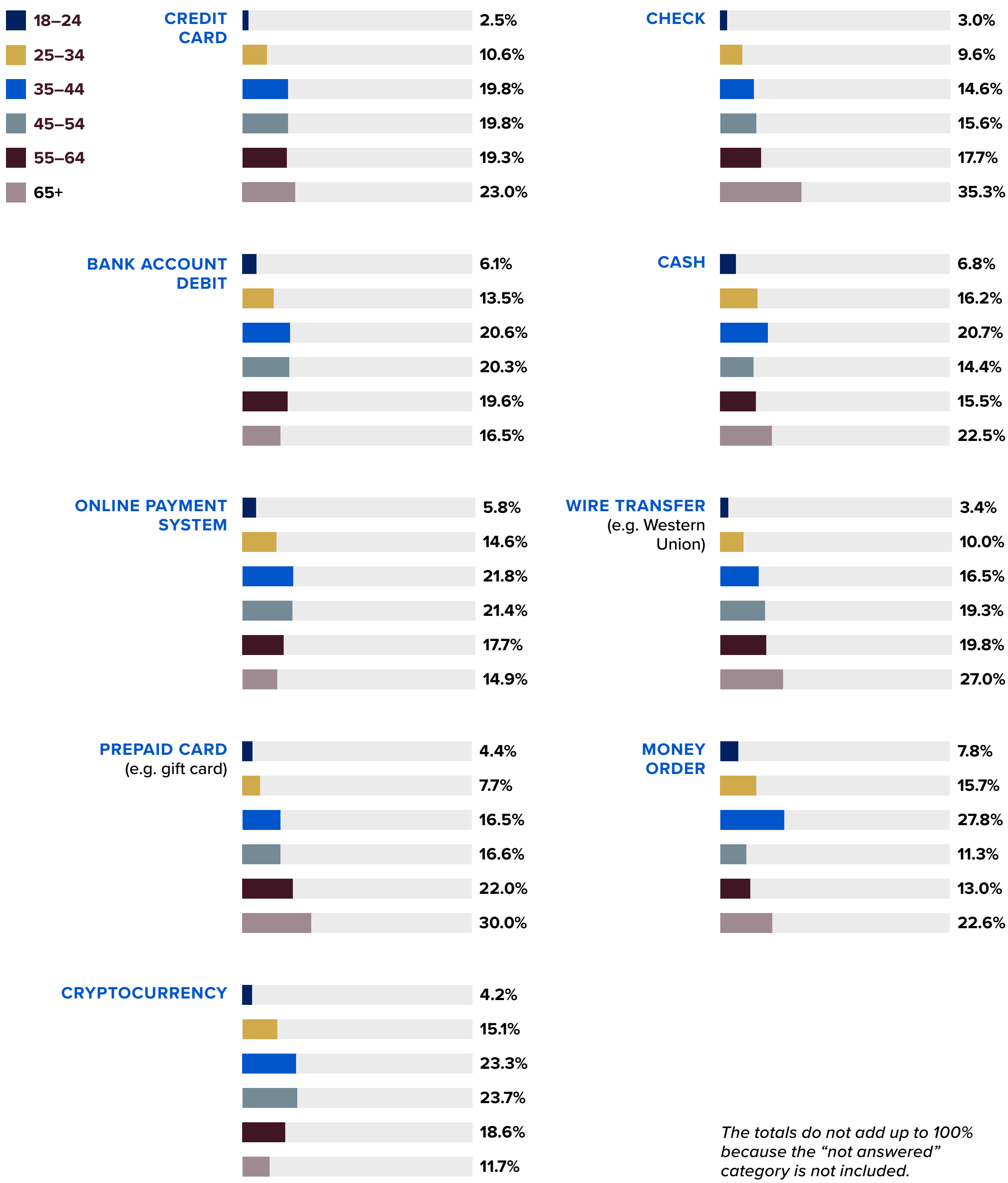
Payment method with a monetary loss

PAYMENT METHOD	% OF REPORTED SCAMS WITH $ LOSS 2025	% OF REPORTED SCAMS WITH $ LOSS 2024	MEDIAN $ LOSS 2025	MEDIAN $ LOSS 2024
Credit card	44.7%	39.4%	$72	$73
Bank account debit	21.6%	22.1%	$70	$85
Online payment system	16.8%	17.1%	$100	$198
Prepaid card (e.g., gift card)	2.1%	3.1%	$400	$500
Cryptocurrency	4.6%	4.8%	$2,800	$3,500
Check	1.7%	2.6%	$1,700	$2,000
Cash	1.7%	2.6%	$800	$1,050
Wire transfer (e.g., Western Union)	1.6%	2.0%	$8,500	$9,000
Money order	0.2%	0.3%	$1,095	$1,563

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

FIGURE 19

Reported payment method with a monetary loss (by age)



The totals do not add up to 100% because the "not answered" category is not included.

TABLE 7

Most reported scam types by payment method

PAYMENT METHOD	NO. 1 MOST REPORTED	NO. 2 MOST REPORTED	NO. 3 MOST REPORTED
Credit card	Online purchase	Counterfeit product	Travel/vacation/ timeshare
Online payment system	Online purchase	Counterfeit product	Employment
Bank account debit	Online purchase	Counterfeit product	Phishing/social engineering
Prepaid card (e.g., gift card)	Online purchase	Phishing/social engineering	Sweepstakes/lottery/ prizes
Cryptocurrency	Employment	Investment/ cryptocurrency	Online purchase
Check	Home improvement	Employment	Online purchase
Wire transfer	Online purchase	Investment/ cryptocurrency	Employment
Cash	Home improvement	Employment	Retail Business

Impact on specific audiences

Canadian consumers

In 2025, Canadian consumers reported 3,201 scams to BBB Scam Tracker (2.2% of total reports submitted in both the United States and Canada). The overall median dollar loss reported in 2025 was CAD$151, down from CAD$311 in 2024. The percentage of those who reported losing money after being targeted by a scam (susceptibility) increased from 59.5% in 2024 to 64.9% in 2025.

The number one riskiest scam type reported in Canada was investment/ cryptocurrency.

The No. 1 riskiest scam reported in Canada was investment/ cryptocurrency scams owing to a high susceptibility (80.8%) and high median dollar loss (CAD$4,354). Home improvement scams rose to No. 2 riskiest, with 81.0% reporting a monetary loss. Employment scams, which made up 16.1% of scams reported in Canada, dropped to No. 3 riskiest (Figure 20).

FIGURE 20

Top three riskiest scams reported in Canada

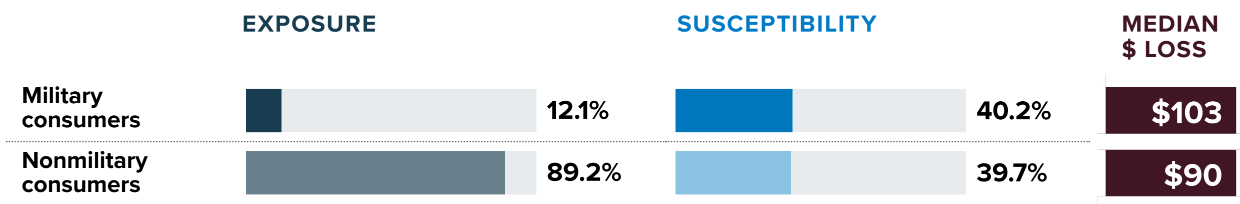
RANK	SCAM TYPE	RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN $ LOSS (CAD)
1	Investment/ cryptocurrency	1220.2	5.2%	80.8%	$4,354
2	Home improvement	759.7	7.1%	81.0%	$2,000
3	Employment	376.8	16.1%	23.5%	$1,500

Military consumers

Military consumers who self-identified as being active-duty military personnel, military spouses, or veterans submitted 12.1% of published reports on BBB Scam Tracker in 2025. In addition, military consumers reported higher median financial losses ($103) than nonmilitary consumers ($90) (Figure 21).

FIGURE 21

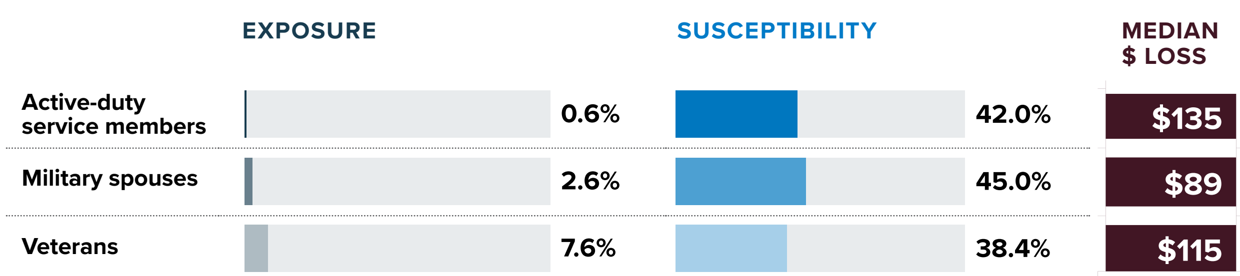
Exposure, susceptibility, median dollar loss (military consumers versus nonmilitary consumers)



We received more reports from veterans than from military spouses and active-duty service members. Military spouses submitted a higher percentage of reports with a dollar loss than veterans and service members (Figure 22). Active-duty service members reported a higher median dollar loss than veterans and military spouses.

FIGURE 22

Exposure, susceptibility, median dollar loss (service members, spouses, veterans)



The BBB Risk Index was applied to identify the riskiest scams for active-duty service members, military spouses, and veterans (Table 8).

TABLE 8

Riskiest scam types: Service members, spouses, veterans

MILITARY TYPE	NO. 1 RISKIEST SCAM	NO. 2 RISKIEST SCAM	NO. 3 RISKIEST SCAM
Service members	Employment	Online purchase	Phishing/social engineering
Military spouses	Home improvement	Online purchase	Employment
Veterans	Investment/cryptocurrency	Online purchase	Employment

Businesses

BBB Scam Tracker collects information about scams that target both consumers and businesses. Businesses reported losing money 18.5% of the time when they were targeted, a lower susceptibility than that reported by consumers (39.8%). The overall median dollar loss reported by businesses dropped from $1,200 in 2024 to $931 in 2025 (Figure 23).

The three riskiest business scams based on the BBB Risk Index include online purchase, fake invoice/supplier bill, and business email compromise scams (Figure 24).

FIGURE 23

Susceptibility and monetary loss resulting from scams reported by businesses

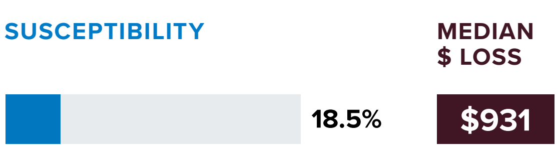


FIGURE 24

Riskiest scam types reported by businesses

RANK	SCAM TYPE	RISK INDEX	SUSCEPTIBILITY	MEDIAN $ LOSS
1	Online purchase	48.7	64.1%	$857
2	Fake invoice/ supplier bill	11.8	6.0%	$532
3	Business email compromise	9.1	12.2%	$5,175
4	Bank/credit card imposter	8.7	3.5%	$9,950
5	Worthless problem-solving service	8.3	32.2%	$1,500

Most impersonated organizations and global brands

Scammers pretend to be well-known companies, brands, and government agencies to perpetrate their scams, co-opting the well-known entities' trust and authority to steal money and information from people. An analysis of reports published on BBB Scam Tracker reveals that PayPal rose to the top of the list of most impersonated global brands reported to BBB Scam Tracker (Table 9). Although this company has been on the list since 2017, this was the first time it landed at No. 1. The Internal Revenue Service was the only government agency to appear in the top 10 in 2025.

PayPal rose to the top of the list of most impersonated global brands reported to BBB Scam Tracker.

Scam types

More than 48% of PayPal impersonation scams were phishing/social engineering scams, followed by credit card (15.3%) and fake invoice/supplier bill (15.2%) scams. Scammers impersonated Amazon to perpetrate employment scams (59.4%), phishing/social engineering scams (15.9%), and online purchase scams (9.1%).

Contact methods

More than 95% of PayPal impersonation scams were perpetrated via email. Amazon impersonation scams were perpetrated in several different ways: text message (56%), phone (23%), email (7%), and social media (6%).

Payment methods

Not surprisingly, 43% of PayPal impersonation scam reports were paid via digital payment app, followed by credit card (16%) and bank account debit (13%). Amazon impersonation scams were paid by credit card (37%), bank account debit (21%), and digital payment app (15%).

TABLE 9

Top organizations and global brands used for impersonation

2025 RANK	2024 RANK	ORGANIZATION/BRAND NAME	NO. OF REPORTS
1	3	PayPal	2,126
2	4	Amazon	1,361
3	—	Target	723
4	—	Warner Brothers Discovery (WBD Global Streaming)	681
5	15	Apple	599
6	1	Publishers Clearing House	488
7	17	Costco	418
8	6	Walmart	310
9	—	Internal Revenue Service	262
10	—	Chase	250

— *Did not appear on the list in 2024.*

Other impersonation trends

Relief checks

Fraudsters distributed phishing messages that promised government stimulus payments to steal personal information or money.

Advance fee loans

Thousands of reports to BBB Scam Tracker highlighted instances of scammers offering advance fee loans in the name of Lending Union West and CNFI USA.

Passport/visa services

More than 500 reports mentioned fake services to help people get passports or visas.

Home warranties

Scammers sent phishing messages pretending to be home warranty businesses claiming the person’s warranty expired and attempting to collect money for services that were not provided.

Toll services

More than 400 scam reports were related to messages that directed people to a website to pay unpaid tolls.

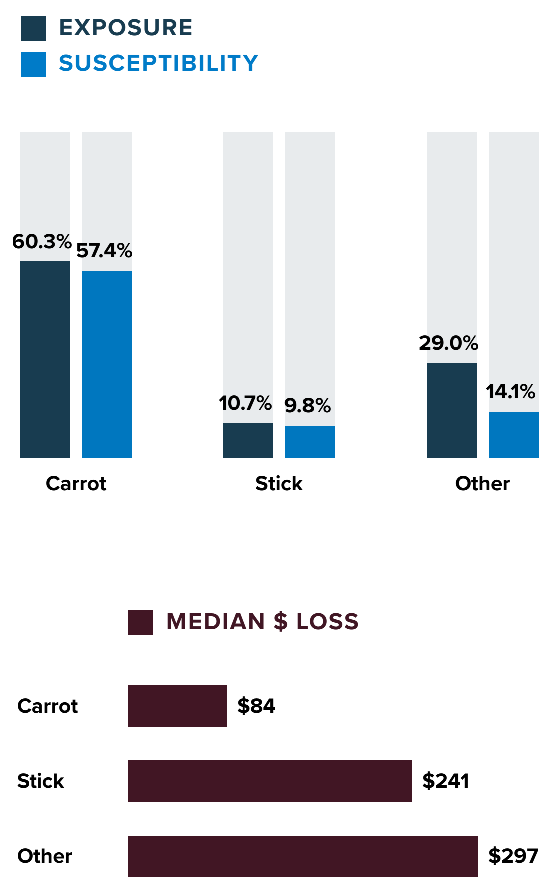
Scammers use threats and opportunities to perpetrate scams

Scammers use a wide variety of tactics to steal money or personal information. Some 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.[9] In Figure 25, 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).

Carrot-type tactics were reported to BBB Scam Tracker the most, making up 60.3% of scams. Stick-type scenarios made up 10.7% of reported scams. Using the BBB Risk Index, we found that when people reported losing money to scams that were perpetrated with a stick method, they reported losing significantly more money ($241) than those who reported losing money to carrot-type scams ($84).

FIGURE 25

Exposure, susceptibility and median dollar loss by tactic (carrot vs. stick)

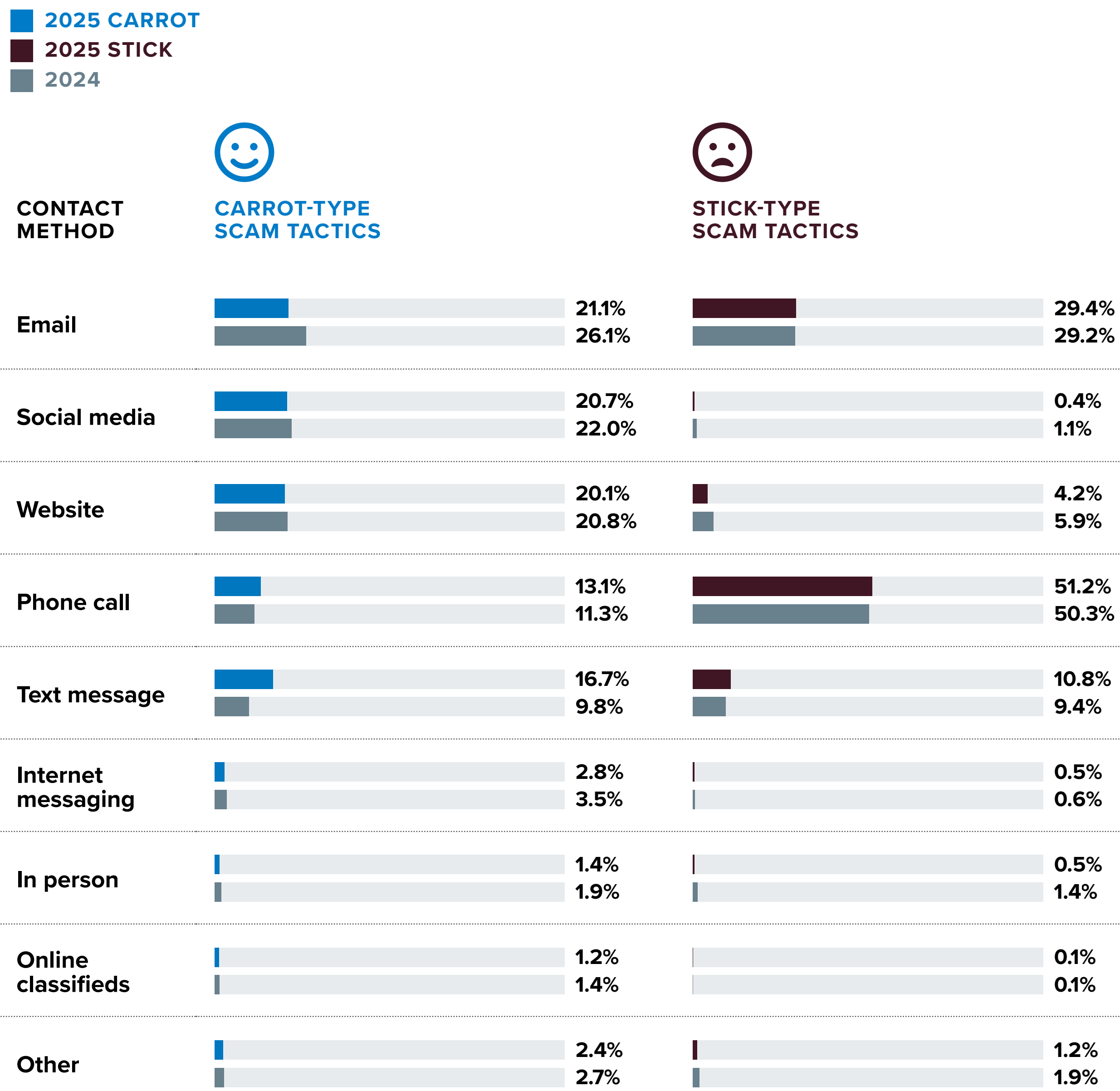


[9] Scams targeting both consumers and businesses were included in this analysis. The breakdown of scam types is as follows:

- **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.

FIGURE 26

Analysis by contact method: carrot-type versus stick-type scam tactics



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

Artificial intelligence and scams

Artificial intelligence is reshaping the online landscape, and scammers are increasingly using AI-enabled tools to support fraudulent activity. However, the role of AI is not always visible to the person targeted by a scam. People who submit reports to BBB Scam Tracker sometimes reference AI directly, though in many cases they are unsure whether artificial intelligence was involved.

AI may be used to strengthen the social-engineering elements of a scam, including drafting persuasive messages, improving grammar, personalizing outreach, creating realistic identities, responding quickly to questions or producing convincing advertisements and websites. Because this use may occur behind the scenes, it can be difficult for consumers—and researchers—to determine whether AI played a role based solely on the final message, image or interaction. Running suspicious content through an AI-detection tool may not provide a reliable answer, particularly when content has been edited, combined with human-written material or generated using different systems.

To better understand how AI may be influencing scam activity, our team analyzed the written narratives in BBB Scam Tracker reports and searched for specific AI-related keywords. This method has important limitations and may capture false positives, including references to automated systems, chatbots and robocalls. It may also undercount scams in which AI was used but not recognized or mentioned by the person submitting the report.

The findings show a notable increase in reports containing AI-related references. This growth may reflect an increase in scams involving AI, greater public awareness and discussion of AI, or a combination of both factors.

AI-related references appeared most frequently in reports involving online purchases, phishing and social engineering, employment, advance-fee loans, counterfeit products, debt collection, and investment or cryptocurrency scams.

The narratives described a wide range of scenarios, including AI-generated or AI-enhanced advertisements, text messages, websites, product reviews and descriptions, videos and images—sometimes featuring public figures or celebrities—and virtual assistants used to market or sell products. A smaller number of reports also described employment scams involving jobs that purportedly required applicants to train AI systems.

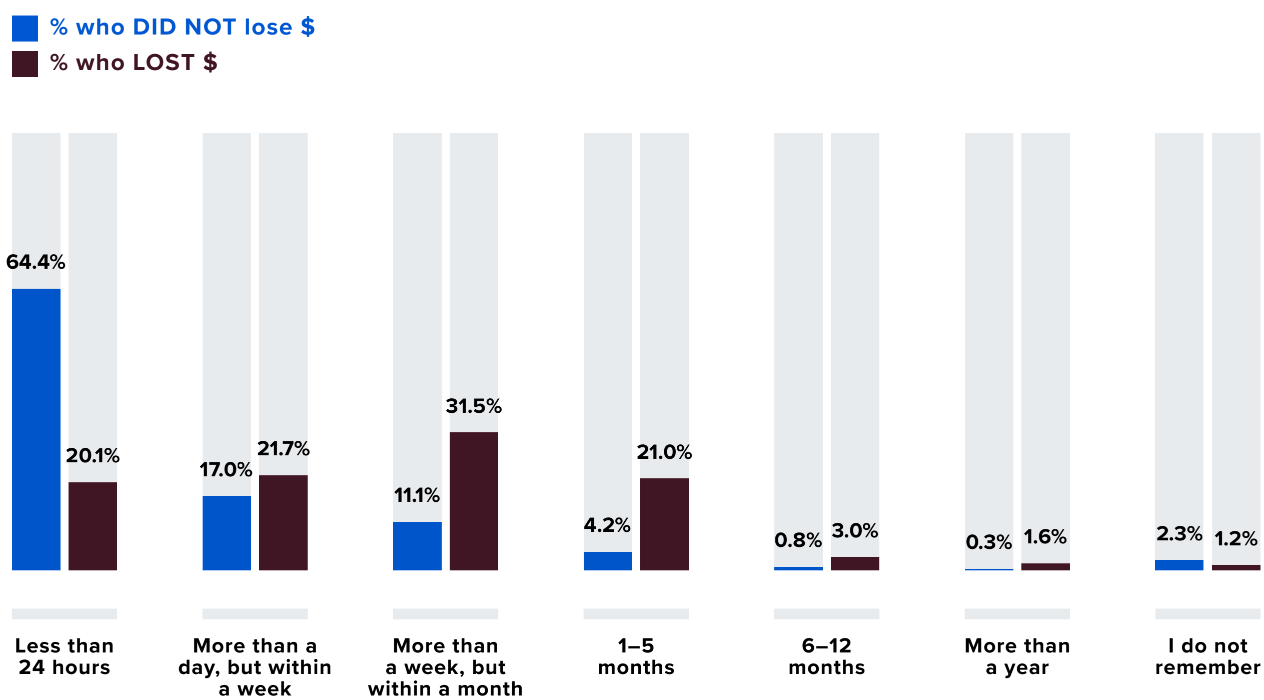
Identifying and reporting scams in the marketplace

Scams have evolved to be more sophisticated and difficult to spot. In some cases, scammers build a relationship with the victim before perpetrating the scam. We asked survey respondents how long it took them to realize the incident was a scam (Figure 27). Those who engaged with the scammer for more than one day were more likely to report losing money.

Those who engaged with the scammer for more than one day were more likely to report losing money.

FIGURE 27

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

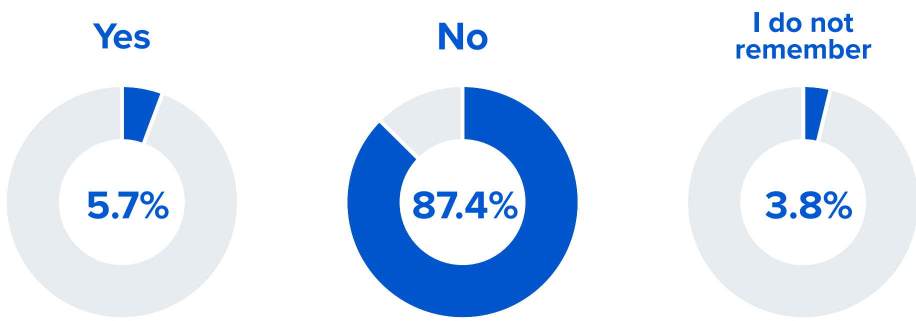


Third party interventions

Many banks, retailers, and other businesses warn customers about potential scams, train frontline employees to intervene if they witness suspicious behavior, post signage, and/or use online messaging that highlights the red flags of fraud. More than 5% of survey respondents said a person, an online message, or posted signage attempted to warn them that a situation might be a scam (Figure 28).

FIGURE 28

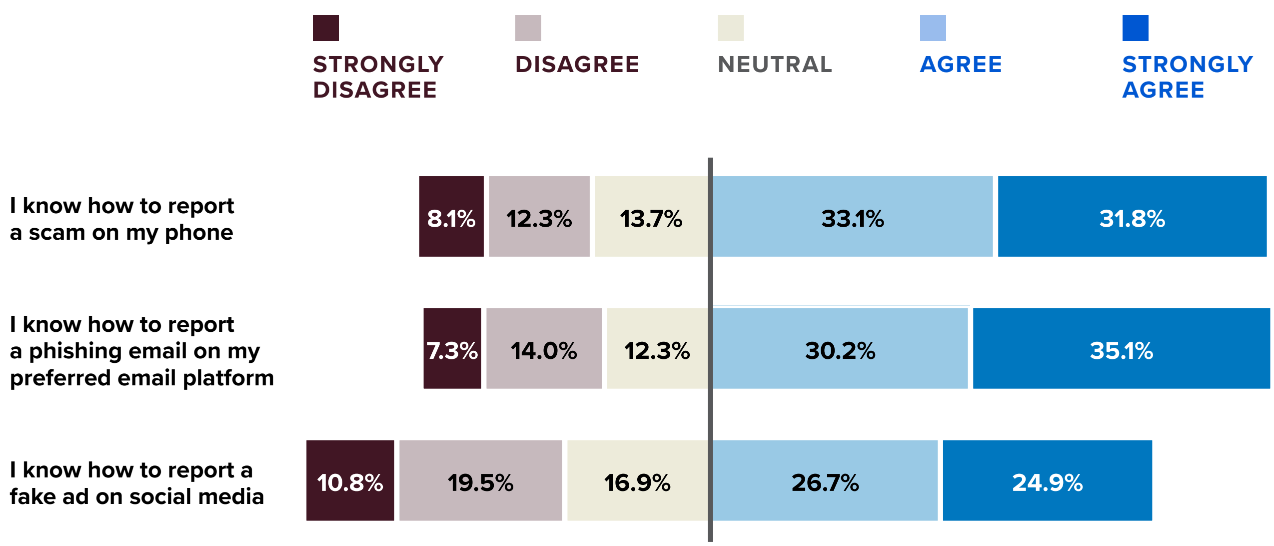
During the scam incident, did a person, an online message, or posted signage attempt to warn you the situation might be a scam?



The responses do not add up to 100% because the “not applicable” category is not included.

FIGURE 29

How much do you agree with the following statements about how to report scams?



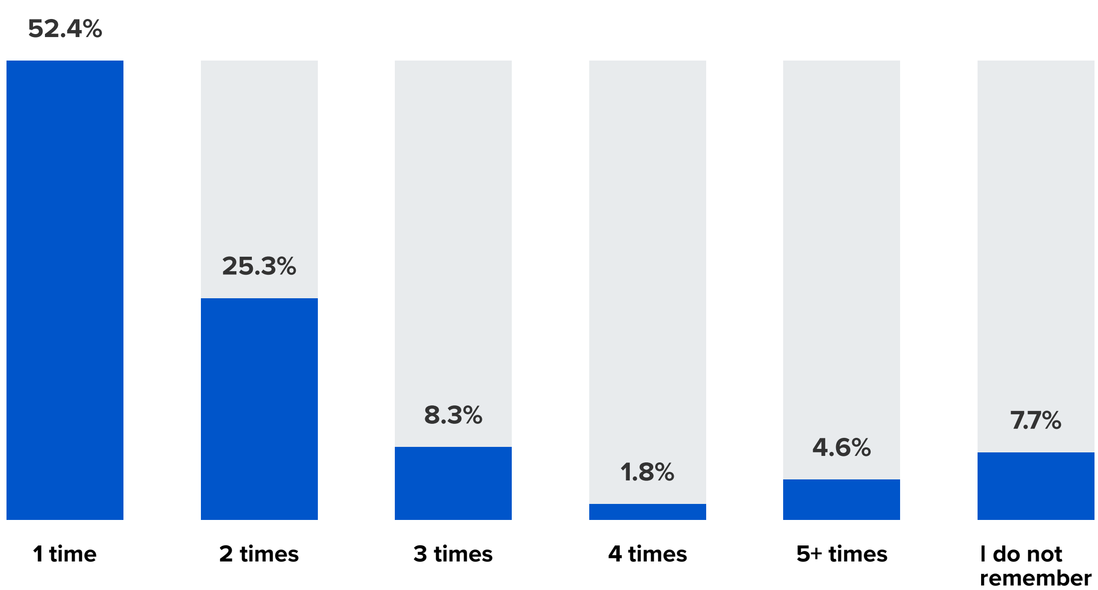
The responses do not add up to 100% because the “prefer not to answer” option is not included.

Repeat victimization

When we asked survey respondents to self-report how many times they lost money to a scam, 14.7% reported losing money at least three times, up from 12.4% in 2024 (Figure 30). Notably, 4.6% reported losing money five or more times, up from 3.8% in 2024.

FIGURE 30

Number of times a person reported losing money to a scam.



Nonfinancial impact of scams

Modern scams are far more complex and technical than the simple cons or impersonation schemes of the past, and that sophistication makes recovery significantly more difficult. Beyond often devastating financial losses, victims may also need support navigating broader consequences, including mental health impacts, debt restructuring, credit repair, and other long-term challenges that extend well beyond the initial scam. When we asked which of these consequences impacted people's lives the most, hurt reputation was considered most impactful, followed by lost earnings and hurt credit health.

Hurt reputation was considered most impactful, followed by lost earnings and hurt credit health.

Figure 31 highlights the nonfinancial impacts people reported after experiencing a scam.[10] We also asked people about the emotional impact of being targeted by a scam (Figure 32).[11] The No. 1 emotion they reported was anger (65.1%), followed by loss of trust (55.8%) and anxiety/stress/trauma (54.4%).

Survey respondents note that the resource they most need following a scam incident is a toll-free scam hotline (47.4%) followed by personalized resources (41.1%) and an online help desk (32.3%) (Figure 33).

[10] A survey was distributed to those who submitted a scam to BBB Scam Tracker in 2025; 2,820 respondents completed the survey.

[11] 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 United States, 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 31

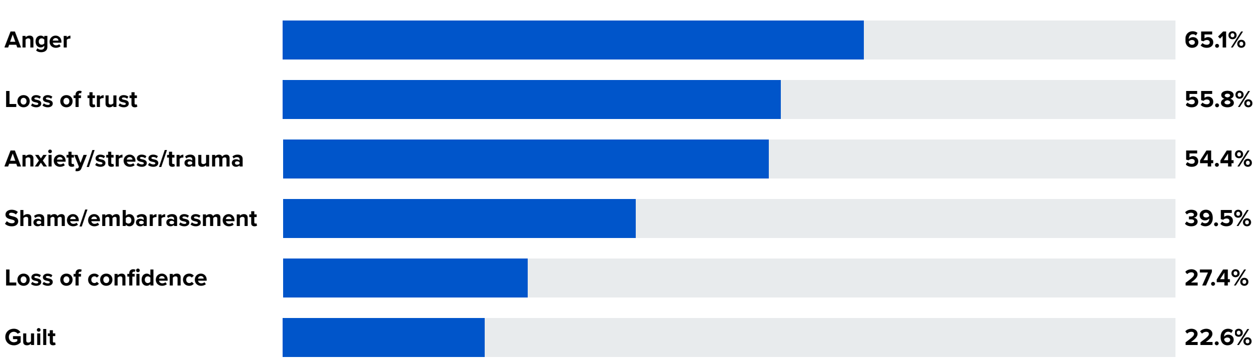
Nonfinancial impact of being targeted by a scam

Time lost	57.1% of reports
Personal information lost	34.9% of reports
Mental health hurt	28.7% of reports
Financial instability	14.0% of reports
Strained relationships	8.0% of reports
Potential earnings lost	7.6% of reports
Credit health hurt	7.5% of reports
Reputation hurt	3.8% of reports

The percentages do not add up to 100% because people could choose more than one answer.

FIGURE 32

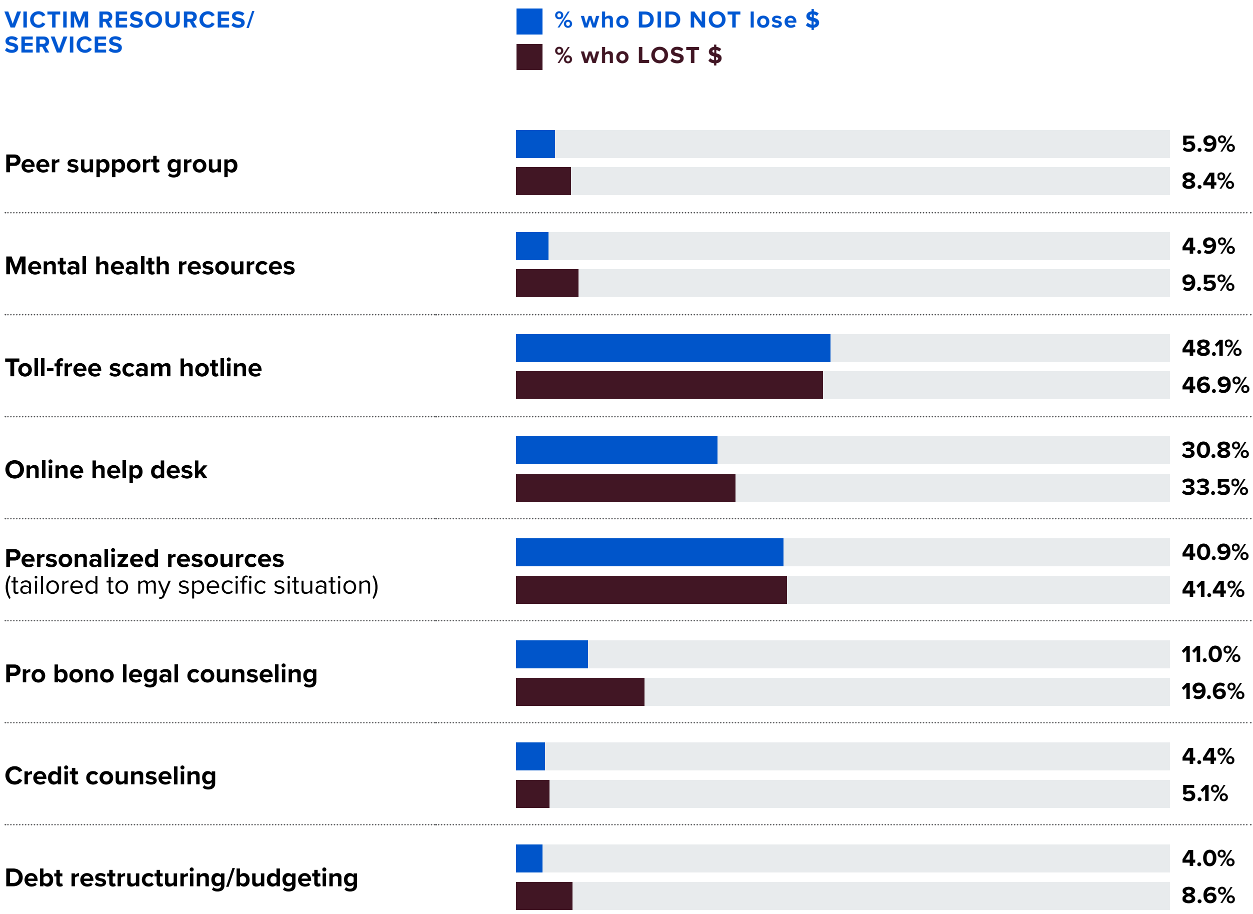
Top emotional impacts of being targeted by a scam (percentage of reports)



These numbers do not add up to 100% because people could choose more than one emotion.

FIGURE 33

Most useful scam victim resources/services



The figures do not add up to 100% because respondents were encouraged to choose more than one option.

10 general tips for avoiding a scam

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

1 Take time to research ads that offer those great deals. Scammers advertise websites that offer low prices but either don't deliver the product or deliver counterfeit products. Search the company name and the word "complaints" online, or enter the company or product name in BBB Scam Tracker, to see if others have reported problems before you make a purchase.

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 online 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.

BETTER BUSINESS BUREAU

10
general tips for avoiding a scam

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

- The offer sounds too good to be true.
- They tell you your bank account is at risk, and you must withdraw your funds immediately.
- The person insists that you must act immediately or that 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 full payment before any 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 **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.

BETTER BUSINESS BUREAU

Learn more 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 advance marketplace trust through education, innovation, and collaboration with our network of BBBs and partners. 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, enabling 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

BBB's *Scam Prevention Guide* helps 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

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**.

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

Thank you to our partners

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

amazon

BBB Better Business Bureau

Capital One

FINRA Investor Education Foundation

Google

JPMorganChase

Microsoft

PayPal

Acknowledgements

BBB Scam Tracker relies on the trust of the 113-year-old BBB brand to collect data from people who have been targeted by fraudsters. This work 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 BBB Scam Tracker, including 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 and Powell River; Tricia Pazsint, director of investigations and advertising for the BBB of Western Pennsylvania; Josh Planos, vice president of marketing, communications & PR for BBB of Midwest Plains; and Lee Anne Lanigan, investigations director for BBB Serving Central Ohio.

We would also like to thank the International Association of Better Business Bureaus for its support of BBB Institute and the *2025 BBB Scam Tracker Risk Report*. We extend a special thank you to IABBB data quality analyst Ryan Hessling for analyzing the BBB Scam Tracker and survey research data for this report.

Project team

Mark Batchelor is the senior director of programs and outreach for the BBB Institute for Marketplace Trust. 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 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* (2023), *Start With Trust Online: Online Scams* (2022), the *Online Purchase Scams Report* (2020 and 2021), the *BBB Scam Tracker Risk Report* (2017–2025), *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.

Appendix A: Glossary of scam types

Scams reported to BBB Scam Tracker this year are classified into specific scam types. 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 **BBB.org/scamtips**.

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 details.
BUSINESS EMAIL COMPROMISE	A scammer impersonates a senior executive via email or another communication vehicle to persuade an employee to transfer payment 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 support legitimate causes. 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 or have just been hired for a promising new job when instead they have given personal information via a fake application or provided money to scammers for "training" or "equipment." The victim may be "overpaid" with a fake check and asked to send back the difference. In a different variation, the victim is hired for an online marketing position and paid via an online account; they are then required to provide their own money to finish the job before they can get their commission or collect their pay. **Read our employment scam prevention tips.**

Appendix A: Glossary of scam types

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 typically target business owners with this scam, hoping they will pay a bill for a product or service they 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 tips on fake invoice scams.**
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.
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.**

Appendix A: Glossary of scam types

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 our 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 scammers will use to gain access to bank accounts or to steal recipients' identity. This type of scheme can also happen within the workplace as an email coming from the CEO, accounting department, or another member of management seeking personal information. **Read our phishing scam prevention tips.**
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/ RELATIONSHIP	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.**
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.**

Appendix A: Glossary of scam types

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 or personal accounts may be accessed. **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 nonexistent advertising or a listing in a nonexistent 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.

Appendix B:
Scam type data table, consumer scams

SCAM TYPE	RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN $ LOSS
Advance fee loan	23.9	4.1%	6.7%	$800
Charity	2.3	0.2%	30.0%	$348
Counterfeit product	23.9	3.1%	90.5%	$80
Credit card	8.4	2.1%	10.7%	$350
Credit repair/debt relief	5.8	0.3%	44.2%	$422
Debt collection	11.7	4.5%	4.8%	$500
Employment	227.4	15.8%	13.3%	$1,000
Fake check/money order	6.2	0.4%	9.7%	$1,474
Family/friend emergency	2.0	0.1%	28.0%	$500
Foreign money exchange	0.0	0.3%	0.3%	$30
Government agency imposter	6.0	1.5%	25.3%	$149
Government grant	7.2	0.2%	22.6%	$1,364
Healthcare/Medicaid/Medicare	7.9	0.8%	18.9%	$483
Home improvement	96.2	0.9%	69.1%	$1,405
Identity theft	6.0	1.0%	29.4%	$181
Investment/cryptocurrency	564.7	1.4%	77.4%	$5,000
Moving	3.6	0.08%	76.1%	$554
Online purchase	185.4	28.4%	89.3%	$68
Phishing/social engineering	41.8	18.2%	6.6%	$325
Rental	9.4	0.3%	65.7%	$415
Retail business imposter	9.4	1.4%	41.0%	$150
Romance/friendship	123.5	0.4%	71.7%	$4,500
Sweepstakes/lottery/prizes	10.3	1.6%	19.8%	$300
Tax collection	0.9	1.4%	1.7%	$350
Tech support	11.5	0.7%	27.8%	$541
Travel/vacation/timeshare	35.3	1.0%	55.8%	$580
Utility	2.0	0.3%	16.8%	$400
Other	34.5	6.1%	34.1%	$155

Appendix C:
Top 10 consumer scam types

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

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

BETTER BUSINESS BUREAU

4250 North Fairfax Drive, Suite 600
Arlington, VA 22203

Institute@IABBB.org

BBB.org/ScamTracker

bbb-institute-for-marketplace-trust