



Scam Red Flags and Avoiding Fraud

By Kelly May

Family Finance and Resource Management

Americans lose billions of dollars each year to fraud. While most people know to beware of offers that sound too good to be true, it is often difficult to tell which offers are truly good and which are bad deals in disguise. The best way to protect yourself from financial fraud and scams is to be aware of the tactics con artists use and learn to recognize red flags so you can avoid being tricked.

Reporting agencies vary on the numbers of fraud victims and dollars lost each year. But they do agree that losses are in the billions per year and that fraud is underreported, which means those losses could be even higher.

Furthermore, fraud can happen to anyone. According to June 2020 data from the Federal Trade Commission's Consumer Sentinel Network, fraud is more often reported by those aged 20-49. However, median dollar losses are much higher for those older than 50, starting at \$300 for ages 50-59, and increasing significantly with each age bracket up to \$1,250 for age 80 and older.



CON ARTIST TACTICS

You cannot tell if a person is a con artist by their appearance. Scam artists come in all ages, sizes, races, and genders. In fact, the “con” in con artist comes from the word “confidence.” The scammer inspires this confidence through their supposed credentials or experience. Also, they often play up their similarities to you to gain your trust.

- **SOURCE CREDIBILITY** is a tactic in which the con artist claims to be with a reputable company. Perhaps the scammer tells you about extensive past experience or may claim credentials, such as special certifications or education certificates. Some credentials take years of study to achieve, while others require little more than a processing fee. To help you research source credibility, FINRA offers a search tool to look up professional designations at <https://www.finra.org/investors/professional-designations>.
- **AFFINITY FRAUD** is a tactic based on trust. The con artist relies on personal similarities to become an accepted member of a group, such as a church, professional, or cultural group. Once they are accepted members, they begin to share their product offer or their supposed “good fortune” with others in the group. In some cases, the group’s leader may fall for the scam, and help spread the word not knowing it is a false offer.
- With the **SOCIAL CONSENSUS** tactic, the scammer makes it appear that you will miss out by not participating. Basically, the scammer tries to persuade you to join in because everyone else is doing it too.
- The **RECIPROCITY** tactic might make you feel like you are getting a bargain, or it might make you feel like you “owe” the seller something for his or her efforts on your behalf. In return for doing you a small favor, the con artist asks you for a bigger



favor. Perhaps they will give you a discount if you buy now or buy a larger quantity. Other times they offer you something “free” in the hopes that you will provide your information or decide to participate later.

- The **SCARCITY** tactic is used to create a sense of urgency. The seller will say that supplies are limited, the opportunity is only open to select members, or the offer is for a limited time only. Perhaps the rush is really so you do not have time to research the facts.
- The **PHANTOM RICHES** tactic is when it truly is “too good to be true.” Examples are guarantees that cannot exist or winning contests without having to enter. The prospect of wealth can be very tempting bait.

Scam artists know how to use your emotions against you. They will ask personal questions until they find something you get emotional about. Then they play up that emotional trigger to get you “under the ether,” according to con artists interviewed in the AARP Publication, “The Con Artists Playbook.” Ether is a heightened emotional state that makes it hard to be rational or think logically. Triggers may include fear, greed, or urgency.

Financial fraud is known to law enforcement as white-collar crime. According to the FBI, it is a financially motivated, nonviolent crime committed by business and government professionals. What makes this crime different is that the con artist tricks you into participating through signing a contract or handing over your money. Through the scammer's trickery, you agree to part with your money.

Fraud makes victims feel bad, not just because they lost money but because they "fell for it." These negative feelings lead people to keep it a secret. Because of this, fraud is underreported and continues to grow. Reporting suspected fraud can help stop scams and keep others from becoming victims.

RED FLAG PROMISES

Besides recognizing tactics a con artist might use, you can also watch out for red flags within the promise, offer, deal, or sale. Some of these red flags include:

- Exclusively for you
- Today only (limited time)
- Only a few left (limited quantity)
- Make the check out to me personally or "cash only"
- Pay by wire transfer, Internet currency, or with a gift card
- Deposit the check, send back some and keep the difference
- Advance payment needed for something you expect to receive (sweepstakes, loan, grant, etc.)
- Contracts with missing or incorrect information
- Will send the paperwork later
- High return, no risk
- "Guaranteed" profits or prizes
- Threatening arrest or legal action
- Requesting your personal information when it is someone who should already have it
- Messages with misspellings or grammar mistakes
- Recorded phone calls that want you to answer "yes" or press 1



Beware of links in emails or text messages. Clicking a link could lead to malware on your device that could leave you exposed to a scammer or hacker. Keep antivirus and other software updated on computers and phones.

While there are people you undoubtedly trust, keep in mind that they could have had their identity stolen. Even those who appear to be your friends and family could be scammers in disguise. Conversely, there is the chance that the friend or family member you really do trust has been a victim and does not know it. Checking out the deal they tell you about could protect you both from fraud.

PROTECT YOURSELF FROM FRAUD

There are two significant ways to protect yourself from fraud. First, decline suspicious offers. Second, research any opportunity.

Offers may come to you in a variety of forms. If it is not something you requested, you do not have to listen. Hang up on calls, delete emails

and texts, block spam calls and emails, do not answer unsolicited door-to-door sales people.

Consider registering on the National Do Not Call List at www.donotcall.gov or 888-382-1222. Be aware, though, that some groups are exempt, and con artists likely will not follow the list. You may still get calls after you register. It may help to come up with a personal “script” for ending unwanted phone calls.

If you are going to consider an offer, take the time to research it. Wait before buying to make sure it is not an emotional purchase. Request all the details in writing, and read the fine print before signing. Provide complete and accurate information on any contract you sign. Ask plenty of questions, and make sure you understand the deal before committing.

Check out the source. Research and verify online businesses before paying. Also, make sure the site is encrypted – look for the “s” in https or a “lock” icon before the web address. If you are hiring someone to help you, check references and verify licenses or credentials. Know your right to cancel if there is one.

REPORT FRAUD

Whether you have been the victim of a scam or your suspicions helped you avoid it, consider reporting potential fraud to authorities. When fraud is not reported, authorities do not have the information needed to stop scams from taking place.

Report suspected scams to the following authorities:

- **Kentucky Attorney General**
at ag.ky.gov/scams or 888-432-9257
- **Federal Trade Commission**
at ReportFraud.ftc.gov or 877-FTC-HELP
- **Better Business Bureau**
at bbb.org/scamtracker

- **Cybercrime – Internet Crime Complaint Center (IC3)** at www.ic3.gov
- **Identity Theft**
IdentityTheft.gov

If you would like to receive text message alerts about current scams in Kentucky, sign up for the Kentucky Attorney General’s Scam Alerts. Text KYOAG Scam to GOV311.

Knowing what to watch for with con artist tactics and red flag promises can help keep you safe from fraud. Knowing where to report fraud can help keep others from falling victim. Hopefully, knowing this information will help you keep your money in your own wallet and out of the hands of a scammer.

Sources and References

- Federal Trade Commission’s Consumer Sentinel Network. “Explore Age & Fraud Loss.” Data as of March 31, 2020. (Retrieved May 28, 2020) <https://public.tableau.com/profile/federal.trade.commission#!/vizhome/AgeandFraud/Infographic>
- Financial Industry Regulatory Authority (FINRA). “Avoid Fraud.” (Retrieved May 28, 2020) <https://www.finra.org/investors/protect-your-money/avoid-fraud>
- FBI. “Affinity Fraud: White-Collar Criminals Use Bonds of Trust to Prey on Investors.” Dec. 18, 2017. (Retrieved May 28, 2020) <https://www.fbi.gov/news/stories/beware-of-affinity-fraud>
- AARP Fraud Watch Network. “The Con Artist’s Playbook: The Psychology Behind ID Theft, Fraud & Scams.” (Retrieved May 28, 2020) https://www.aarp.org/content/dam/aarp/money/scams_fraud/2013-10/The-Con-Artists-Playbook-AARP.pdf