Scam Awareness and Protection

By Jessica Gaehle, Student Intern

Introduction, definition, and statistics

Elder fraud is defined as the illegal, improper, or deceptive use of an older adult's (60+) funds, assets, or property for another's monetary gain (FBI Elder Fraud website et al., n.d.). In 2025, over 200,000 individuals aged 60 and older reported losses totaling more than $7 billion to the FBI's Internet Crime Complaint Center (IC3). In the same year the IC3 reported victims aged 60+ lost an average of more than $38,000 and More than 12,000 people aged 60 years and older lost over $100,000 (FBI Elder Fraud website et al., n.d.).

These statistics are not meant to cause fear or panic, but to highlight that fraud is common and that anyone can be targeted by scammers, regardless of educational level or background. As technology advances, identifying scammers' schemes becomes increasingly more difficult to recognize. It is important to recognize that being a victim of fraud is not shameful or your fault; the responsibility lies with the people who commit these harmful acts. Informing yourself about potential scams you could be exposed to, how to protect yourself and your loved ones, and what to do when you suspect or are a victim of fraud, is a pivotal step to defending yourself and your loved ones against different fraudulent scams.

Types of scams to be aware of

There are numerous types of scams to be aware of. According to the FBI Internet Crime Complaint Center, there are 6 common fraud schemes to be mindful of.

The first being investment fraud. This scheme has stolen over $3 billion from those over the age of 60. Investment fraud is when an individual (the criminal) offers you, by phone, email, or advertisement, unsuitable investments, fraudulent offerings, or unrecognizable or intangible products.

The second most common scam is tech and customer support, which has led to the total loss of $1 billion. This scam occurs in different ways. The first being when a criminal poses as someone from tech support offering assistance for a nonexistent issue, like your bank accounts being hacked, or a computer/phone virus. Criminals may also pose as customer support for lost packages or for faulty products and services sending messages that claim there is an issue and include a link for you to click. Clicking on those links will give the criminal access to the device you are actively using.

The third most common scam for those 60 and older is a romance scam. This is when a criminal poses as an individual interested in you romantically on social media or on dating websites or apps. These individuals will often ask for money or gifts over a period of time; usually, the amount of money or gifts requested will increase over time. These criminals will not always directly ask, but will use tactics to either guilt-trip or induce a sense of need or urgency for money through telling stories of tragedy or never having enough money. The criminal will often stay in contact with the victim until they are no longer able to pay the criminal's demands or requests.

The fourth most common scam is the grandparent/emergency scam. The criminal in this instance will pose as a close relative, usually a child or grandchild, who will claim to be in immediate financial need.

The fifth most common scam is government impersonation, which has led victims to lose $413 million in total. Scammers will impersonate various governmental officials; most commonly, they will impersonate representatives from the IRS, Social Security Administration, law enforcement, and Medicare. Scammers will typically use threats of arrest or prosecution until the victim agrees to pay a set amount of money or give personal information. Scams will induce a sense of fear, panic, and urgency.

Lastly, the sixth most common scam that victimizes those 60 years old and older is sweepstakes, lottery, and inheritance scams. The perpetrator will contact victims, stating that they have won a sweepstakes, lottery, or that a distant or unknown relative has left them an inheritance. The scammer will then tell the victim that to claim the money, they either need to pay fees, taxes, or provide personal information like banking information.

How to Protect Yourself and Your Loved Ones

A great line of defense against scams is to place your phone number and your loved ones' numbers on a no-call registry. There are national and state no-call registries. These registries are free to use and provide a permanent list that stops most legitimate sales calls. They are helpful because if you still receive sales or investment calls after registering, you can recognize them as likely fraudulent since legitimate companies are no longer permitted to contact you. The National No-Call Registry is linked below at the end of this article.

Another useful tool is a credit freeze. A credit freeze is a free request that prevents any of the credit bureaus from sharing your credit reports with any lenders. This prevents identity thieves from opening any accounts or lines of credit/loans in your name. This does not impact your credit score; it is free to do and undo, and you can still use any already open accounts and credit lines. A credit freeze is done through one or all of the three major credit bureaus: Equifax, Experian, and TransUnion. A credit freeze can be conducted on any of the credit bureaus' websites, which are linked below.

Scam callers can and will still contact you and your loved ones even when registered on the No-Call list. When these calls occur, here are a few tips to follow. First, when answering the phone, instead of saying “yes”, say “this is she/he”. This can deter scam callers from making a recording of your voice to pose as you for use in contacting banks or other institutions with your personal name.

The second tip is implementing Pause, Reflect, and Protect (About AARP Fraud Watch Network, 2026). Scammers induce a sense of urgency, fear, and sometimes panic to steal your money. When these emotions occur, that is a “red flag” or a sign that this could be a scam call. When this occurs, it is best to **pause** and give yourself time to calm down and avoid acting on the emotion. Next, **reflect**, think about what the caller is telling you, and reflect on whether what they are saying makes sense. Is it legal? Is it really who they claim to be? You can also search the phone number listed on the call to see who it is registered under.

Lastly, you want to **protect** yourself once you reflect and suspect that the call is a scam. Protect yourself by hanging up the phone and blocking that number. It is also recommended that you follow the tips above (No-Call Registry and Credit Freezes).

If you or a loved one is a potential victim of cyber-enabled fraud, file a complaint with the IC3 and contact your local Attorney General.

Memory Keepers is here to help! We can provide resources, answer questions, and offer other services. Contact us at info@MemoryKeepers.org

Helpful links

- National No-Call Registry
  - https://www.donotcall.gov/
- Some States also have their own No-Call Registry
  - There is no one location for these registries; it is recommended you search if your state has a No-Call Registry
- National Elder Fraud Hotline and How the Hotline Works
  - https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope#no-fear-total-understanding
- Contact your local attorney general's office
  - https://www.naag.org/attorneys-general/
    - This website can help you find your Attorney General and answer questions about their role.
  - Missouri's Attorney General
    - https://ago.mo.gov/
  - United States Attorney General
    - https://www.justice.gov/ag
- File a complaint with the Internet Crime Complaint Center (IC3)
  - https://www.ic3.gov/
- The Federal Trade Commission has an online report for fraud
  - https://reportfraud.ftc.gov/
- Credit Bureaus links to implement a credit freeze
  - **Equifax**: https://www.equifax.com/personal/credit-report-services/credit-freeze/
  - **Experian**: https://www.experian.com/help/credit-freeze/
  - **TransUnion**: https://www.transunion.com/credit-freeze
- Fraud alert information
  - https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts#fraud_alerts
- How to be safe on the internet and how to file a report with the FBI
  - https://www.fbi.gov/how-we-can-help-you/scams-and-safety/on-the-internet
- Information on Cyber-enabled Fraud and different types of scams
  - https://www.ic3.gov/Outreach/Brochures/elder_fraud_tri-fold.pdf
- Federal Trade Commission: Information on scams and tips to stay safe
  - https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings
- The AARP has a multitude of resources for scams and a hotline
  - https://www.aarp.org/money/scams-fraud/about-fraud-watch-network/