Vanguard

Stay vigilant, protect your finances, and avoid exploitation

What is financial exploitation?

Financial exploitation occurs when someone illegally or improperly gains access to your assets through theft, deception, intimidation, or undue influence. Financial exploitation collectively costs clients billions annually.

Who is at risk?

Anyone—but retirees are often targeted because of their accumulated wealth.

Where does exploitation happen?

Scams and exploitation happen over the phone, through mail or email, or over the internet. They can also occur in person, at your home, or at a business. Awareness is the first step in planning your financial well-being.

What are commons scams and their warning signs?

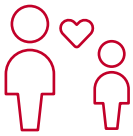
Romance scam

The criminals who carry out this scam are experts at what they do and will seem genuine, caring, and believable.

- The person you're dating is far away on business.
- Their profile seems too good to be true.
- The relationship is moving fast.
- They break promises to visit.
- They ask for money (wires, gift cards, etc.).

Tech support scam

- A pop-up message or blank screen usually appears on a computer or phone, telling you that your device is compromised and needs fixing.
- When you call the support number for help, the scammer may either request remote access to your computer and/or require you to pay a fee to have it repaired.



Grandparent scam

- Scammers will place a call to an older person and say something along the lines of: "Hi Grandma/Grandpa, do you know who this is?"
- When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity without having done any background research.
- Once "in," the fake grandchild will ask for money to solve some unexpected financial problem (overdue rent, car repairs, jail bond) and will beg the grandparent not to tell anyone.

Government impersonation scam

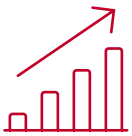
- Caller pretends to be from the Internal Revenue Service (IRS), Social Security Administration, or Medicare.
- They may say you have unpaid taxes and threaten arrest or deportation if you don't pay up immediately. Or they may say your Social Security or Medicare benefits are in danger of being cut off if you don't provide personal identifying information (that can then be used to commit fraud).
- Government impersonators often "spoof" the actual phone numbers of the government agency or call from the same zip code.

Sweepstakes/charity/lottery scam

- Here, scammers inform their mark that they've won a lottery or sweepstakes of some kind and need to make some sort of payment to unlock the supposed prize.
- Often, seniors will be sent a check they can deposit in their bank account, knowing that while it shows up in their account immediately, it will take a few days before the (fake) check is rejected.
- During that time, the criminals will quickly collect money for supposed fees or taxes on the prize, which they pocket while the victim has the "prize money" removed from their account as soon as the check bounces.

Family/caregiver scam

- These trusted individuals try to gain control of a senior's money, assets, and credit. They also may withhold needed care to retain control over the person and their assets.
- Seniors who have a disability or cognitive impairment (such as dementia) may be at particular risk.



Investment scams

- These scams involve promises of big payouts, guaranteed, or overly consistent returns. Always be suspicious of any investment opportunities that promise a high return with little or no risk.
- Before making any investment related decisions, take your time, avoid high-pressure sales pitches that require you to act now or lose out.

For the most up-to-date scam alerts visit FTC.gov

Common ways scammers will attempt to separate you from your money:

- Request that you wire funds to an unknown party.
- Ask for gift cards or cash.
- Request access to your devices to then take over your accounts.
- Require a fee/taxes to send you a prize/winnings.
- Offer deals that are good for today, or pressure you to act quickly.

If it sounds too good to be true, it probably is.

Don't be afraid or ashamed to talk about it with someone you trust.

You're not alone, you've done nothing wrong, and there are people who can help.

- Call your financial institutions to inform and update all security measures on your account.
- Open all your mail, even if you think it's junk. Ensure accounts or credit aren't being established in your name.
- Contact credit bureaus if your personal information has been compromised.
- Consider placing a temporary freeze on your credit and compromised accounts to allow time to get account security measures in place and/or updated.
- Report to IC3.gov for online scams and FTC.gov for all scams.
- File a police report.
- Screen calls and insist on verifying callers you don't know who are asking you for personal or financial information.
- If you're concerned that a loved one may no longer be capable of managing their own finances, talk to their physician, understand what documents may already be in place (power of attorney), and obtain assistance from an attorney who specializes in elder law.
- If you are not near a loved one who you believe is being taken advantage of, consider reporting your concern to adult protective services in their county.

What proactive steps can you take to protect yourself from a future event?

1. Consider creating an estate plan.

Talk with an attorney who can help you create a will, power of attorney, financial power of attorney, or health care directive.

2. Set up a trusted contact on your account.

To protect your assets, create a plan while you're in good health. Start by talking to a trusted family member, professional, or friend about your wishes for your finances. Naming a trusted contact on your account can offer additional protection by:

- Allowing us to reach out to someone you trust if we're concerned about your well-being or believe you're being financially exploited.
- Assisting us in identifying and contacting your power of attorney or legal guardian.
- Helping ensure we're informed if you develop a medical condition—especially forms of dementia such as Alzheimer's disease—and are no longer able to protect your interests.

We recommend selecting someone who will be able to provide an informed assessment of your whereabouts, well-being, and health status. Also, consider naming someone who can't transact on your accounts to help ensure objectivity.

3. If managing your finances becomes too difficult or you could just use some help, consider asking someone you trust to support you.

If you don't have anyone, consider hiring a professional.