



Scammers swindled at least \$3.4 billion from Americans aged 60 and older in 2023. This figure represents the average loss experienced reported by elder fraud victims, while the true extent of losses is likely much higher.

Even more alarming are the sophisticated tactics employed by these scammers. Elder fraud manifests in various ways, including phone, text, and email scams, as well as internet fraud.

This resource guide provides valuable information to help you navigate the complexities of financial exploitation. It offers tools to protect your hard-earned assets and maintain your financial independence.

Let's come together in the fight against fraud, ensuring our elders can live with security and dignity.

Bill Gladson, State Attorney

TABLE OF CONTENTS

COMMON SCAMS ————————————————————————————————————	01
FOUR SIGNS That let you know its a SCAM	03
PHISHING No, we aren't talking that kind - Phishing Emails or Text Messages	04
TELEMARKETING The old but tried and true way of scamming	05
PROTECT & MONITOR Keep a close eye on your credit report and protect yourself	06
MENTAL & EMOTIONAL EFFECTS ————————————————————————————————————	09
PROTECT YOUR LOVED ONES Scammers with a convincing story are closer than you think	10
RESOURCE GUIDE Resources available to you	11

COMMON SCAMS TARGETING OLDER ADULTS

Most scams use three tactics: scammers contact you unexpectedly; they create a sense of urgency; they provide a specific way to pay or send money.

GOVERNMENT IMPOSTER SCAMS

An imposter scam starts with a call, email, text, or social media message from someone who says they're with a government agency, business, or charity. They use spoofing to appear as if they are calling from an official phone number. They might provide an "ID number" or have information about you. They'll give you a legitimate-sounding reason why you need to send money or give them your personal information immediately.



IRS IMPOSTER SCAMS

The caller claims you owe taxes you must pay immediately. They might threaten to arrest you if you don't pay right away.

SOCIAL SECURITY IMPOSTER SCAMS

The scammer says your benefits will end, or your Social Security number will be suspended, unless you pay immediately.





MEDICARE & MEDICAID FRAUD

Scammers pose as insurance agents, offer "help" with Medicare enrollment, and trick victims into sharing personal information.

TECH SUPPORT IMPOSTER SCAMS

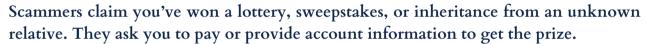
Scammers call or use fake security pop-up messages and claim your device has a virus or your accounts were hacked. They fool you into handing over money or personal information.



TELEMARKETING & ROBOCALL SCAMS

Most telemarketing scams bypass the Do Not Call registry using robocalls and prerecorded messages. These scams use spoofing to falsify the information transmitted to your caller ID display. Examples include imposter scams, debt relief and credit repair scams, business and investment scams, extended car warranties, and charity scams.

SWEEPSTAKES/LOTTERY & INHERITANCE SCAMS







INVESTMENT SCHEMES

Scammers lure victims into investing in fraudulent or non-existent opportunities, promising high returns with little or no risk.

ROMANCE SCAMS

Criminals adopt a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.



HOME REPAIR/CONTRACTOR SCAMS

The caller claims you owe taxes you must pay immediately. They might threaten to arrest you if you don't pay right away.

EMPLOYMENT SCAMS

Job seekers are lured with false promises of lucrative positions or work- from-home opportunities. Scammers often request personal information or upfront payment for training or equipment, but the job never materializes. Sophisticated scammers often create fake websites and emails that closely resemble trusted brands and businesses.



SIGNS, THAT IT'S A SCAME SCAME STATE SIGNS, THAT IT'S A SCAME STATE STATE

Criminals use sophisticated tactics to trick potential victims into disclosing personal and financial information. Typically, they use these P's – Pretend, Problem or Prize, Pressure, and Payment.

Scammers PRETEND to be from an organization you know.

Scammers might say they are contacting you on behalf of the government, such as the FTC, Social Security Administration, IRS, or Medicare. Some pretend to be from a business you know, like a utility company, a tech company, or a charity. They use technology to change the phone number on your caller ID. The name and number you see might not be real.

2 Scammers say there's a PROBLEM or PRIZE.

They might say you're in trouble with the government, owe money, someone in your family had an emergency, or there's a virus on your computer. Some might say there's a problem with one of your accounts and that you must verify information. Others will lie and say you won a lottery or sweepstakes but must pay a fee.

3 Scammers PRESSURE you to act immediately.

Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story. They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

Scammers tell you to PAY in a specific way.

They often insist that you can only pay by using cryptocurrency, wiring money through a company like Money Gram or Western Union, using a payment app, or putting money on a gift card and then giving them the numbers on the back of the card. Some will send you a check (that will later turn out to be fake), then tell you to deposit it to send them money.

PHISHING EMAILS TEXT MESSAGES

Phishing occurs when a scammer, masquerading as a trusted entity, tricks a victim into opening an email, pop-up message, or text message.

COMMON INDICATORS OF PHISHING

- Offers that seem too good to be true
- High-pressure sales pitches that stress urgency
- Alerts that there is a problem with an account
- Shortened or misspelled links
- Emails that don't address you by name
- Messages with poor grammar and spelling
- Direct requests or demands for payment
- Requests to confirm personal information

TELEMARKETING SCAMS

In 2022, seniors lost \$724 million to imposter and tech support scams originating from call centers. Unwanted calls - including illegal and spoofed robocalls - are the Federal Communications Commission's top consumer complaint.

HOW TO AVOID THESE SCAMS...

- •Never send money or give out personal information such as credit card numbers, bank account. numbers, birthdays, or Social Security numbers to unfamiliar companies or unknown individuals.
- •Research unfamiliar businesses and services.
- •Request documentation about an offer or charity.
- •Do not be pressured into making a decision or payment
- •Never pay for a "free prize."
- •Pay for services only after they are delivered.
- •Be cautious of companies that want to send a messenger.
- •Understand that your personal information is often brokered through third parties.
- •Report suspected fraud immediately to local, state, or federal law enforcement agencies.



Identity theft can happen to anyone, but you can reduce the risk of becoming a victim by taking some simple steps to protect your personal information.

STOP MAIL FRAUD AT THE MAILBOX



Informed Delivery is a free service from the U.S. Postal Service that emails photos of your expected letter-size mail. It helps prevent mail theft by identity thieves. Pick up your mail promptly.



HALT SCAMMERS AT YOUR DOOR

The caller claims you owe taxes you must pay immediately. They might threaten to arrest you if you don't pay right away.

PREVENT GARBAGE THEFT



Shred receipts, credit offers, loan and credit applications, insurance forms, bank statements, and similar documents when you no longer need them. Take advantage of community shredding events.

AUDIT YOUR WALLET

Leave your social security card and Medicare card at home – unless you are going to need them for a specific reason.





WATCH FOR CREDIT CARD SKIMMING

Credit card skimmers capture data from the magnetic stripe on credit cards. Use chipenabled cards or contact-less payment methods when possible. Inspect card readers for tampering or loose parts. Notify a cashier immediately, and pay with another method.

PROTECT YOUR FINANCIAL ACCOUNTS



Every few months, revise the passwords on your financial accounts and consider using a passphrase. Ilovemy17dogz! is much stronger than Scruffy23. Keep track of passwords in a highly secure password manager. Or, write them down and store them safely at home.



SECURE YOUR COMPUTER

Turn on two-factor authentication for secure websites. Use an anti-virus software service. Paid subscriptions include ad tracker blocking, cloud backups, and identity theft monitoring.

SAFEGUARD YOUR SMARTPHONE

If you have a newer phone, turn on biometric identification (fingerprint or facial recognition). Set up your phone to send calls from unknown numbers to voicemail. Sign out of financial apps when you aren't using them. This includes apps for credit cards, banks, and peer-to-peer apps including Venmo, CashApp, or Zelle.





PROTECT YOUR EMAIL ACCOUNTS

Designate unsolicited and unwanted emails in your inbox as spam, so future emails from that site get blocked. Do not open file attachments in emails from businesses or people you don't trust completely. Malware is often planted via email attachments.

SET LIMITS ON SOCIAL MEDIA



Set your Facebook profile so only your friends can see your page. Click the downward arrow button in the upper-right corner of your Facebook account, then click on Settings & Privacy and Privacy Checkup. Never accept friend requests or respond to messages from people you don't know.



VERIFY ONLINE STORES

Check the spelling of websites. Scammers often create a URL with one letter off from the authentic one and hope you won't catch it. Remove your credit card information from restaurant delivery and retail sites. Pay using a secure e-payment service.

MONITOR YOUR CREDIT REPORT

Free weekly online credit reports are available from Equifax, Experian and TransUnion. The reports are available at AnnualCreditReport.com - the only source for free credit reports authorized by Federal law.

AnnualCreditReport.com

If you think you have been a victim of identity theft:

- Contact your bank(s) and credit card companies immediately.
- •File a police report.
- •Contact one of the three credit bureaus to place a fraud alert. A fraud alert is free and will make it harder for someone to open new accounts in your name.

EXPERIAN

1-888-EXPERIAN (1-888-397-3742) www.Experian.com/fraudalert

<u>EQUIFAX</u>

1-888-766-0008

www.Equifax.com/CreditReportAssistance

TRANSUNION

1-800-680-7289

www.TransUnion.com/fraud



MENTAL EMOTIONAL EFFECTS OF FRAUD

Financial fraud doesn't just impact your bank account. The crime can also impact a victim's mental and physical health. Some fraud victims become too anxious to leave the house, too ashamed to talk to close friends, or too jaded to explore new relationships.

ANXIETY

You might feel vulnerable, and imagine others as dangerous, deceptive, and harboring malicious intentions. Anxiety can exacerbate cognitive decline, elevate blood pressure, affect cardiovascular health, weaken the immune system, and lead to risky coping behaviors.

SHAME

You might feel embarrassed about being scammed and hesitant to share details with loved ones because you fear they will question your wisdom or try to restrict your financial independence.

GRIEF

You might grieve the loss of your financial security, sense of independence, or trust in people. If you were the victim of a romance scam, you might grieve the loss of that relationship. You might also cycle through feelings of anger, despair, and numbness.

PROTECT YOUR LOVED ONES FROM.

Scams and fraud by strangers can happen even in protected places like assisted living communities and nursing homes.

Scammers with a convincing story are as close as the telephone, the mailbox, or the computer.

SIGNS TO LOOK FOR...

- •A large amount of money is missing from their bank account(s).
 - •Numerous withdrawals of smaller amounts, such as \$100 at a time.
 - •A large check written to someone you do not know.
- •A change in power of attorney or insurance and investment beneficiaries.
- •A caregiver or "friend" who is overly interested in the older adult's finances or blocks access to them.
 - •A change in power of attorney or insurance and investment beneficiaries.
 - Bounced checks or unpaid bills.
- •Unusual or unnecessary purchases or home repairs.
- •Piled up sweepstakes, mailings, magazine subscriptions.

RESOURCE CUDE

There are a number of ways to report fraud or suspected fraud at the local, state, and national level. The Federal Trade Commission (FTC) provides several online reporting tools for a variety of fraud. If you are unsure of what type of fraud to report, use the "Report Fraud" website below.

ReportFraud_fte_gov

Identity Theft

Create an Identity Theft Report by filing a report with the FTC. Your Identity Theft Report proves to businesses that someone stole your identity, and makes it easier to correct problems caused by identity theft.

- IdentityTheft.gov
- **•**1-877-438-4338

Internal Revenue Service (IRS)

If you get an IRS notice in the mail that says someone used your Social Security number to get a tax refund, follow the instructions provided in the letter. Report suspected IRS phone scams to the Treasury Inspector General for Tax Administration:

Federal Deposit Insurance Corporation (FDIC)

The FDIC does not send unsolicited correspondence asking for money or sensitive personal information, such as bank account information, credit and debit card numbers, Social Security numbers, or passwords.

- •1-877-ASK-FDIC or 1-877-275-3342
- •ask.fdic.gov

Social Security Related Scams

To report a Social Security related scam:

- •1-800-772-1213 or 1-800-325-0778 (TTY)
- •ssa.gov/scam



If your Social Security card was lost or stolen, you can apply online for a free replacement card:

•ssa.gov/ssnumber

For Social Security benefits, contact the SSA Office of the Inspector General:

- •oig.ssa.gov
- •1-800-269-0271

Replace Government IDs

Contact your nearest motor vehicles office to report a lost or stolen driver's license. The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a replacement card. Find your nearest motor vehicles office:

•usa.gov/Motor-Vehicle-Services

If your passport is lost or stolen, contact the State Department:

•1-877-487-2778 or TTY 1-888-874-7793

Charity Scams

If you are unfamiliar with a charity, the State of Florida's help line can verify if it is registered with the state.

•1-800-HELP-FLA

Internet Crime Complaint Center (IC3)

File complaints about online crimes, including cryptocurrency investment schemes, ID theft, credit card fraud, ransomware, business email compromise scams, financial fraud, romance scams, lottery/ sweepstakes scams, and more.

•ic3.gov

Do Not Call Registry

- •1-888-382-1222
- •TTY: 1-866-290-4236
- donotcall.gov



Elder Options

Elder Options' mission is to ensure that communities have a trusted and unbiased place to turn for information, resources and assistance.

- •1-800-262-2243
- •agingresources.org

Florida State Attorney General Scam Reporting

The Florida Attorney General's Office issues consumer alerts about emerging scams, new methods used to commit fraud, trends in consumer complaints, or other deceptive practices utilized to take advantage of Floridians.

•myfloridalegal.com/consumer-protection

File a scam complaint:

- •1-866-9NO-SCAM or 1-866-966-7226
- •myfloridalegal.com

<u>Jury Duty Phone Scam (Marion County)</u>

A court official will never ask for you to wire money or ask for your confidential information over the phone or via email. If you suspect you are the victim of a jury duty scam, hang up and report the call to the Marion County Clerk's Jury Office.

Fifth Judicial Circuit State Attorney's Office

The Office of the State Attorney has trained Victim Witness Specialists dedicated to supporting crime victims. These specialists help victims understand their legal rights and protections, providing assistance during the overwhelming aftermath of crime.

- •352-671-5800
- •sao5.org

Marion Senior Services

Marion Senior Services is a nonprofit, charitable social agency providing supportive care services to elderly, disabled, and disadvantaged residents of Marion County, Florida.

- •352-620-3501
- •marionseniorservices.org

Marion County Sheriff's Office

The men and women of the Marion County Sheriff's Office are committed to meeting the needs of our growing senior community with integrity and respect. MCSO's Seniors At Risk Assistance (S.A.R.A.) program is designed to give law enforcement the opportunity to provide personal contact with persons who live alone or have special needs that should be aware of in order to better serve and protect them.

- •352-369-6745
- •marionso.com

Ocala Police Department

Seniors vs. Crime is an exceptional initiative led by the Florida Attorney General's Office in collaboration with OPD. Its primary objective is to provide assistance to seniors and individuals facing issues with service providers and contractors. Unfortunately, some seniors, particularly newcomers to our community, have fallen victim to dishonest vendors.

- •352-873-6377
- •ocalapd.gov/resources/victim-services/senior-vs-crime



Florida Department of Elder Affairs

The FDOEA strives to promote the well-being, safety, and independence of Florida's seniors, their families, and caregivers. The office offers information about its programs and services to those who wish to apply.

- •1-800-96-ELDER (1-800-963-5337)
- •elderaffairs.org

NOTES

NOTES

