To report abuse of an elder or dependent adult
by a business or scam, please contact:
Riverside County Adult Protective Services
24-Hour Hotline

1-800-491-7123

RIVERSIDE COUNTY
DEPARTMENT OF PUBLIC SOCIAL SERVICES
ADULT SERVICES DIVISION C.A.R.E. PROGRAM

DPSS 4361 (Rev. 11/2020) CARE: When Trust is a Weapon

WHEN TRUST
IS A WEAPON

C.A.R.E. PROGRAM
COUNTY OF RIVERSIDE DEPARTMENT OF PUBLIC SOCIAL SERVICES
ADULT SERVICES DIVISION

RESOURCES & REPORTING GUIDE

When and How to Report Elder and Dependent Adult Abuse

WHAT CAN YOU DO TO HELP COMBAT ELDER & DEPENDENT ADULT ABUSE?

Elder Abuse affects all of us.
Together, we can make a difference.
If you observe, have knowledge of, are told about,
or reasonably suspect abuse, take the time to report it!

HOW DO YOU REPORT?

Call Riverside County Adult Protective Services
Available 24-hours a day, 7 days a week

APS Hotline: 800-491-7123

If an emergency, or if a crime is in progress, call 911 and then call APS!
You may choose to remain anonymous;
however, all reports remain confidential.

TYPES OF ABUSE:

Physical, Financial, Abduction, Abandonment, Isolation,
Emotional, Neglect and Self-Neglect

C.A.R.E. PROGRAM
COUNTY OF RIVERSIDE DEPARTMENT OF PUBLIC SOCIAL SERVICES
ADULT SERVICES DIVISION

Table of Contents

When Trust is a Weapon:
Elder Fraud Prevention and Consumer Awareness

The truth is, anyone can fall victim to a scam as criminals are always looking for new ways to take advantage of those in our community. They seek to gain a person's trust and keep them engaged, because without their participation, they could not do what they do. It is precisely the individual's trust they must rely on to use it as weapon against them. Be informed and empower yourself and others around you to be prepared when approached in person, by phone, text, email, or mail.

As the population of older adults increases, so do scams targeting this growing population. Falling victim to scams and other acts of financial exploitation can have a far-reaching impact on one's overall mental and physical health. The best way to protect yourself from fraud is to be aware and practice strategies that keep you and your money safe.

The C.A.R.E. (Curtailing Abuse Related to the Elderly) Program with Riverside County Department of Public Social Services, Adult Services Division, serves older adults (65 years+) and dependent adults (18-64, unable to carry out normal activities of daily living due to a mental/physical limitation) who are victims of fraud by businesses or strangers. C.A.R.E provides advocacy to guard and regain assets, and offers support and assistance to prevent further abuse, all while preserving the client's confidentiality and dignity.

RESOURCES & REPORTING GUIDE

Federal Trade Commission (FTC) (877) 382-4357 (877) 438-4338 www.ftc.gov	Contact FTC to report fraudulent debt collection practices, lottery/sweepstakes fraud, and identity theft.
FINRA (Financial Industry Regulatory Authority) (800) 289-9999 www.sss.finra.org	Contact FINRA to verify if investment consultants are licensed and to report fraudulent investors.
Health Insurance Counseling and Advocacy Program (HICAP) (800) 434-0222 www.HICAP.org	HICAP provides free assistance with Medicare, HMO, and long-term care insurance.
Inland Counties Legal Services (ICLS) (800) 977-4257 (For Seniors) (888) 245-4257 (Toll Free) (888) 455-4257 (Housing Hotline for Landlord/Tenant Issues) https://www.inlandlegal.org	ICLS provides free legal services for low income seniors regarding civil law issues, such as landlord/tenant disputes, trusts, and family law.
Medical Board of California, Central Complaint Unit (800) 633-2322 www.med.bd.ca.gov	Contact the Medical Board to report complaints and receive information about physicians.
Medicare (877) 772-3379	Contact Medicare to report Medicare Drug Plan Scams or to ask questions about prescription drug plans.
National Fraud Information Center www.fraud.org (800) 876-7060	Contact the National Fraud Information Center to report fraud and get information on internet fraud and telemarketing scams.
Network of Care https://portal.networkofcare.org/Sites/california	Network of Care is a comprehensive, internet-based tool which provides a wealth of resources for older adults and persons with disabilities.
Office on Aging (800) 510-2020 www.rcaging.org	Contact the Office on Aging for free information and referrals on senior services available throughout the county.
Opt-Out (888) 567-8688 www.optoutprescreen.com	The Opt-Out service prevents your credit file from being given to companies for credit offers.
Riverside Legal Aid (951) 682-7968 Riverside office (760) 347-9456 Indio office www.riversidelegalaid.org	Riverside Legal Aid is a non-profit organization that helps with legal issues for residents of Riverside County.
Securities and Exchange Commission (SEC) (800)-732-0330 www.sec.gov	Contact the SEC to report fraudulent practices and check the licenses of investment consultants/brokers.
Social Security Administration (SSA) (800) 772-1213 www.socialsecurity.gov	Contact the SSA to obtain information regarding Social Security benefits, and to order a free copy of your earnings and benefits statement to check for identity theft.

RESOURCES & REPORTING GUIDE

C.A.R.E. Program **Riverside County Adult Services** (800) 491-7123 (24 hrs. 7-days a week) CARE@Rivco.org	The C.A.R.E. Program provides advocacy for elder and dependent adult victims of consumer fraud by businesses and conducts free educational trainings on elder abuse including scams.
Charities - BBB Wise Giving Alliance (703) 276-0100 www.give.org	Check the BBB Wise Giving Alliance to verify the validity of a charity.
CONNECT IE www.connectie.org	Search CONNECT IE for free or low-cost services, such as medical care, food, job training, and more.
Contractor's State License Board (CSLB) (800) 321-2752 www.cslb.ca.gov	Contact CSLB to verify a contractor's license and file a complaint.
Credit Report (Free Annual Services) (877) 322-8228 www.annualcreditreport.com	Individuals can request an annual credit report from all three credit agencies to identify and/or prevent I.D. theft.
CVHIP.COM www.CVHIP.com	Coachella Valley Health Info Place (CVHIP) is a free, one-stop website to find community resources in the Coachella Valley.
Department of Financial Protection and Innovation *(Formerly Department of Business Oversight)* (866) 275-2677 https://dfpi.**ca**.gov	Contact the Department of Business Oversight to report fraudulent practices and check the licenses of investment consultants/brokers, as well as report fraudulent practices by corporations.
Department of Motor Vehicles (DMV) (800) 777-0133 www.dmv.ca.gov	The DMV Investigations Division protects the programs and interests of the department and public through active fraud/counterfeit detection, investigation, audit and enforcement services.
District Attorney's Office, Riverside County (951) 955-5400 www.rivcoda.org	The District Attorney's Office is the legal entity for criminal prosecution for Riverside County
DMA Mail Preference Service P.O. Box 634 Carmel, NY 10512 https://dmachoice.org	Contact the DMA Mail Preference Service to reduce unwanted mail advertisements.
Do Not Call Registry (Telemarketing) www.donotcall.gov	Contact the Do Not Call Registry to remove your contact information from telemarketing call lists.
Fair Housing Council of Riverside County Riverside: (951) 682-6581 Moreno Valley: (951) 658-8314 Palm Springs: (760) 864-1541 www.fairhousing.net	The Fair Housing Council of Riverside County, Inc. (FHCRC) takes part in a variety of activities to fight housing discrimination, such as free educational workshops, outreach to the community, and the investigation of discrimination complaints.

Charity Fraud

Americans contributed nearly $450 billion to various charities in 2019 according to the Giving USA Foundation's annual report on U.S. philanthropy. This act of generosity supports many amazing organizations which put those billions to work for health care, education, environmental protection, the arts and numerous other causes. Unfortunately, it also opens a door for scammers, who capitalize on donors' goodwill to line their pocket.

Many such frauds involve faux fundraising for veterans and disaster relief. Scammers know how readily we open our hearts and wallets to those who served and those rebuilding their lives after hurricanes, earthquakes or wildfires. They also follow the headlines. The spread of the novel corona virus in early 2020 was accompanied by phony appeals to donate to victims or emergency response efforts.

But charity scams come in all shapes and sizes, from gifts on social media and crowdfunding sites to massive national cons, like the network of bogus cancer charities the Federal Trade Commission (FTC) said cheated donors nationwide out of $187 million before it was prosecuted in 2015.

Sham charities succeed by mimicking the real thing. Like genuine nonprofits, they reach you via telemarketing, direct mail, email and door-to-door solicitations. They create well-designed websites with deceptive names. For example, as hurricanes churn toward landfall, for example, scammers snap up URLs featuring the storm's name. Some operate fully outside the law; others are in fact registered nonprofits yet devote little of the money raised to the programs they promote.

Charity scammers are especially active during the holidays, the biggest giving season of the year. However, with a little research and a few precautions, you can help ensure your donations go to organizations which genuinely serve others, instead of helping themselves.

—

Charity Fraud

Warning Signs —

- Pressure to give right now. A legitimate charity will welcome your donation whenever you choose to make it.

- A thank-you for a donation you don't recall making. Making you think you've already given to the cause is a common trick unscrupulous fundraisers use to lower your resistance.

- A request for payment by cash, gift card or wire transfer. Those are scammers' favored payment methods because the money is difficult to trace.

— DOs —

- Do check how watchdogs like Charity Navigator, CharityWatch and the Better Business Bureau's Wise Giving Alliance rate an organization before you make a donation. Contact your state's charity regulator to verify the organization is registered to raise money there.

- Do your own research online. The FTC recommends searching for a charity's name or a cause you want to support (like "animal welfare" or "homeless kids") with terms such as "highly rated charity," "complaints" and "scam."

- Do pay attention to the charity's name and web address. Scammers often mimic the names of familiar, trusted organizations to fool donors.

- Do ask how much of your donation goes to overhead and fundraising. One rule of thumb, used by Wise Giving Alliance, is at least 65 percent of a charity's total expenses should go directly to serving its mission.

- Do keep a record of your donations and regularly review your credit card account to make sure you were not charged more than you agreed to give or unknowingly signed up for a recurring donation.

— DON'Ts —

- Don't provide personal and financial information, such as your Social Security number, date of birth or bank account number to anyone soliciting a donation. Scammers use such data to steal money and identities.

RESOURCES & REPORTING GUIDE

211 **Riverside County Community Connect** www.211.org	Dial 2-1-1 for toll free, confidential service providing Riverside County residents access and referrals to community and health information 24 hours a day, 7-days a week and in many languages.
AARP www.aarp.org (888) 687-2277	**Americans Association of Retired Persons** AARP is our nation's largest nonprofit, nonpartisan organization dedicated to empowering Americans 50 and older to choose how they live as they age.
Adult Protective Services (APS) **Riverside County** (800) 491-7123 (24 hrs. 7-days a week)	Call APS hotline to report suspected abuse of an elder or dependent adult. Types of abuse include physical, financial, sexual, emotional, abandonment, isolation, abduction, neglect and self-neglect.
Attorney General of California (916) 445-9555 www.oag.ca.gov	Contact the Attorney General's office to report consumer complaints against a business. Online reporting is also available.
Bar Association (951) 682-1015 Riverside area (760) 346-4741 Desert area www.desertbar.com www.riversidecountybar.com	Contact the Bar Association to request referrals for attorney assistance in Riverside County.
Better Business Bureau (BBB) **www.bbb.org/us/ca** (800) 675-8118	Contact the BBB to file complaints against or obtain information about businesses. The BBB can also provide standard quote ranges on home projects.
Bureau of Automotive Repair Dept. Consumer Affairs (800) 952-5210 www.bar.ca.gov	The Bureau of Automotive Repair will investigate auto repair problems and can mediate on your behalf.
California Department of Consumer Affairs (800) 952-5210 www.dca.ca.gov	Contact the Department of Consumer Affairs to report fraudulent debt collection agencies.
California Department of Housing and Community Development (800) 952-8356 www.hcd.ca.gov	HCD helps to provide stable, safe homes affordable to veterans, seniors, young families, farm workers, people with disabilities, and individuals and families experiencing homelessness. HCD assists mobile homeowners with registration renewal, residency law protection, mobile home fee and tax waivers and buy, sell, or transfer instructions.
California Department of Insurance (800) 927-4357 www.insurance.ca.gov	Contact the Department of Insurance to research insurance and annuity products, as well as the agents who sell them.
California Bureau of Real Estate (877) 373-4542 www.dre.ca.gov	Contact the Bureau of Real Estate to report fraud or verify the credentials of real estate professionals.

Work-at-Home Scams

— DON'Ts —

- Don't assume a work-at-home offer is on the level because you saw it in a trusted newspaper or on a legitimate job website. It could still be a scam. If you spot a suspicious listing, report it to the publication or site.

- Don't believe website testimonials. Fake work-at-home sites are full of personal stories of people (often struggling, single moms) making thousands of dollars a month because they took advantage of this amazing opportunity.

- Don't sign a contract or make a payment without doing homework about the company making the offer.

- Don't stick around if there's any suggestion that your earnings are based primarily on recruiting other people to join the operation — it's probably a pyramid scheme.

Information provided by AARP

REPORT SCAMS

If you believe you've responded to a scam, file a complaint with:

- **Federal Trade Commission**
- **State Attorney General**

Charity Fraud

- Don't make a donation with cash, by gift card or wire transfer. Credit cards and checks are safer.

- Don't click on links spouting fundraising messages in unsolicited email or from other social media platforms, such as Facebook or Twitter. They can unleash malware (malicious software).

- Don't donate by text without confirming the phone number on the charity's official website.

- Don't assume pleas for help on social media or crowdfunding sites, such as GoFundMe, are legitimate, especially in the wake of disasters. The FTC warns that fraudsters use real victims' stories and pictures to con people.

-Information provided by AARP

Distraction Burglaries

A distraction burglary happens when you are home, and you play a role in it. Typically, it involves at least two suspects. A person (suspect) will park in your driveway or near your home. Usually a work truck will be visible. The suspect will claim to be from a company that provides some type of repair service. They may attract you to the outside of your house to see where the repair is needed. They may attract you to the basement of your home, to see where a repair on your water tank or HVAC is needed. In the meantime, a second suspect or group of suspects enters your home and takes your valuables. Additional suspects could be in the truck or in another vehicle nearby. The victim then discovers the missing property and the suspects are long gone. Most times, the involved truck will be unmarked. It may lack a front license plate. It may block the rear plate by leaving the tailgate down or otherwise obstructing it. The suspect usually will not have ID or a business card.

The best advice here is if you don't recognize the company as a local company, and you did not call them to your home, be very careful. Definitely do not let them in your house, not even to use the bathroom. Do not go outside with the suspect. Tell the person that you are too busy and ask for their business card. Tell them that you can call them and schedule a better time. You can call the police and report when they leave if you really think it was suspicious.

APS HOTLINE 800-491-7123

Grandparent Scam

The grandparent scam has been around for years. The victim receives a phone call from someone who claims to be their grandchild. The perpetrator will state there is an emergency and they need money sent to them quickly, often through wire transfer or gift cards. The caller will request the grandparent to not discuss the call with other family members out of embarrassment.

The caller may have gathered information regarding the victim from social media sites, hacked into an email account, or purchased a list of potential targets. The caller will supply the victim with enough pertinent information to make them believe the caller is their relative. The caller may use a second person to act as an authority figure, such as a policeman or lawyer to make the situation seem more authentic.

People receiving a call such as this are advised to avoid panicking. Don't let the urgency of the call pressure you into making a hasty decision. Avoid wiring money to someone you do not know, and without confirmation of an emergency. Police officials and other reputable businesses will never ask for payment in the form of gift cards. Instead, take the time to reach out to your relatives and verify the authenticity of the story. Ask the caller for a call back number. Most scammers will not provide one and will terminate the call.

To try and avoid calls such as this, place privacy settings on your social media accounts and install antivirus software on your computer and other devices.

Work-at-Home Scams

— Warning Signs —

- A job ad claims that no skills or experience are required
- It offers high pay for little or no work
- A company promises that a business opportunity is surefire and will pay off quickly and easily.
- You're required to pay upfront for training, certifications, directories or materials.

— DOs —

- Do check out the company offering the job with your state consumer protection agency, and with the Better Business Bureau in your community and the area where the company is located.
- Do learn about the FTC's Business Opportunity Rule, which requires companies to disclose key information about business opportunities they are selling, to provide references and to back up claims about how much you can earn.
- Do ask detailed questions, such as these that the FTC recommends:
- How will I be paid? By salary or by commission?
- Who will pay me, and when will the checks start?
- What is the total cost of the program, and what will I get for my money?
- Do check that job sites, specializing in remote work, screen the openings and companies listed.

Work-at-Home Scams

Identifying work-at-home scams can be tricky, especially as they often appear alongside legitimate opportunities on popular job-search websites. If you're a retiree looking to supplement your Social Security, or a worker left reeling by a late-career layoff, it can be awfully tempting to follow those leads. Who wouldn't like to earn big money stuffing envelopes or posting online ads from the comfort of your couch or get all of the tools and training needed to start a lucrative home-based business? Few of these offers ever lead to actual income. Instead, they're liable to leave you with a lighter bank account or even heavily in debt.

From 2015 through 2019, the Federal Trade Commission (FTC) received more than 58,000 consumer complaints about scam opportunities to work from home or launch a business. The median loss for victims is about $1,200, according to the Better Business Bureau's BBB Scam Tracker, which says employment frauds pose the highest scam risk for military services members and veterans.

Typical ploys invite you to get to work stuffing envelopes, processing billing forms for medical offices, filling out online surveys, doing typing or data entry, or assembling crafts. The common thread is that you'll be asked to pay something upfront for supplies, certifications, coaching or client leads. In return you may get a load of useless information, or nothing at all, or a demand that you place more ads to recruit more people into the scheme.

More involved cons promise to set you up in an online business — again, for a price, which can rapidly escalate into the thousands of dollars as one paid "training program" leads to another. One such operation, a Malaysian company called My Online Business Education, agreed in February 2020 to settle claims that it defrauded thousands of would-be entrepreneurs with costly business-coaching programs before being prosecuted by the FTC.

There are genuine work-from-home jobs out there. The trick is knowing how to spot the real opportunities in a sea of empty — and costly — promises.

Healthcare Scams

The route to getting the right health coverage can seem like a bewildering bureaucratic maze, especially since the advent of the Affordable Care Act (ACA). Shady operators count on this confusion, allowing them to sell you insurance products and health services that deliver far fewer benefits than promised, or none at all.

These scams proliferate when health care is in the news and on consumers' minds — for example, during the annual open enrollment periods for ACA and Medicare. Fraudsters try to convince you they have a simple solution to the complexity and expense of getting coverage. They "cold-call" potential victims or generate leads through websites offering information about "comprehensive" health plans that meet ACA requirements. Some feature the names and logos of major insurers, or even AARP. People who respond are peppered with pitches promising full coverage with low premiums, deductibles and co-pays.

The resulting policies turn out to be, at best, skimpier than advertised or, at worst, outright fakes. Often victims are buying medical discount plans, in which consumers pay a monthly fee to get reduced prices from participating medical providers. Some discount programs are legitimate, but as the Federal Trade Commission (FTC) warns, they are not a substitute for insurance. In November 2018, the FTC filed a complaint against a Florida company that allegedly defrauded more than $100 million from consumers by dressing up discount-plan memberships as comprehensive coverage, leaving buyers uninsured and often stuck with big medical bills.

During ACA enrollment, which runs from November 1st to December 15th in most states, scammers routinely impersonate representatives of the government-run Health Insurance Marketplace. They tell you they need personal information to verify an application or that they can help you choose the right plan, for a fee. Treat such solicitations, and any offers of deep-discount coverage, with a healthy dose of skepticism.

— Warning Signs —

- High-pressure sales pitches that push low-cost plans or offer special rates if you sign up right away.

- Claims that a plan is licensed under ERISA, the federal Employee Retirement Income Security Act. Insurance companies are licensed by the states, not by any federal body.

Healthcare Scams

- A plan requires you to join an “association” or “union” in order to receive coverage. These may be fake organizations designed to create the illusion that you are buying group health insurance.

- Someone contacting you about health coverage claiming to be from the government. No government representative will ever try to sell you insurance.

— DOs —

- Do compare rates. Premiums for “comprehensive” coverage that are far lower than what you see elsewhere are probably too good to be true.

- Do confirm with your state insurance commissioner that a plan provider is licensed.

- Do insist on seeing a statement of benefits or a complete copy of the policy.

- Do learn about the difference between medical discount plans and health insurance, and ask specific questions to make sure you know what you’re getting.

- Do research an association or union named in an insurance pitch. Look for a U.S. street address and phone number, and for evidence of activity other than selling health insurance.

- Do research if an unfamiliar company says it sells plans through a major insurer like BlueCross BlueShield. Research before agreeing to any terms or conditions.

Technology Scams

Tech scams are becoming more and more common as people that use a computer at home age into the senior community. These seniors are familiar with technology, but their use of technology makes them vulnerable to scammers. The following scams are some of the most common affecting our seniors:

- Computer Takeover: The senior is browsing the internet and a pop-up appears indicating their computer has an issue. The senior is instructed to call the scammers at the phone number listed in the pop-up. The senior then grants the scammer access to their computer and the scammer locks the victim’s computer with a password. The scammer holds the victim’s computer hostage until the victim pays the scammer, and the scammer removes the password requirement.

- Computer Software Purchase: Similar to the computer takeover, the senior receives a pop-up on their computer indicating they lack a computer security software, i.e. a firewall or anti-virus, and they need to call the number listed on the pop-up. When the senior calls the number, they are given options to purchase with the most expensive option being the “best” deal. The victim “purchases” a temporary “protection plan” and grants the scammer access to their computer. The scammer then claims to be adding the software to the computer by opening programs in the victim’s computer, leaving the victim, a satisfied customer, primed for the next phase of the scam.

- Computer Software Refund: Now that the victim has purchased the “protection plan” the scammer calls back, telling the victim they are due a refund because they paid too much for the software. The scammer will claim that the victim paid around $200-500 too much. The victim logs into their online banking and grants the scammer access to their computer. The scammer then moves a large sum of money from the victim’s savings account and puts it in the victim’s checking account. For example, if the victim was “due” a $200 “refund” the scammer will move over $2,000 and tell the victim they accidentally refunded too much money. The scammer will then instruct the victim to wire the $1,800 difference to them so they don’t lose their job. The scammer will have cheated the victim out of thousands of dollars by the end of the scam.

Tech scams can be avoided by ignoring the messages in the pop-ups, closing the pop-ups, not calling phone numbers you have not sought out, and not granting anyone remote access to control your computer for any reason.

Social Security Scams

Social Security numbers are the skeleton key to identity theft. And what better way to get someone's Social Security number than by pretending to be from Social Security?

The Scam: A common tactic involves fake SSA employees calling people with warnings that their Social Security numbers have been linked to criminal activity and suspended. The scammers ask you to confirm your number so they can reactivate it or issue you a new one, for a fee. This is no emergency, just a ploy to get money and personal data. Social Security does not block or suspend numbers, ever.

This con is sometimes executed via robocall - the recording provides a number for you to call to remedy the problem. In another version, the caller says your bank account is at risk due to the illicit activity and offers to help you keep it safe.

In another scenario, you might get a call from a supposed SSA representative bearing good news - say, a cost-of-living increase in your benefits. To get the extra money, you must verify your name, date of birth and Social Security number. Armed with those identifiers, scammers can effectively hijack your account, asking SSA to change the address, phone number and direct deposit information on your record, thus diverting your benefits.

Other types of scams may include: The alleged Social Security Administration caller tells you that the government has a case or lawsuit against you. Or scammers leverage the growing threat of data breaches and identity theft to try to convince you that your Social Security number has been compromised.

How do you know it's a scam? Because the government says so. The Social Security Administration doesn't suspend, revoke, block or freeze Social Security numbers. The agency wouldn't call you about anything other than personal matters, like benefits claims. The Social Security Administration does not ask taxpayers to wire funds or send money in the form of gift cards.

How to not be a victim: If you do answer the phone and the caller demands money, hang up — don't give out personal information.

Who do you report Social Security fraud to? If you suspect a person or organization of social security fraud, contact the Office of the Inspector General at SSA. You can contact the office by mail, phone, or call SSA's Fraud Hotline (1-800-269-0271). Cases of identity theft should be reported to the Federal Trade Commission.

Healthcare Scams

— DON'Ts —

- Don't enter personal information on a website in exchange for a price quote. You are likely setting yourself up for identity theft or a barrage of sales calls.

- Don't keep talking to a sales agent who gives vague or evasive answers to coverage questions or tells you the details are "in the brochure."

- Don't sign up for a plan if the bar for acceptance seems too low - for example, if you are not required to get a physical or provide a medical history. Some scam sites claim you can get insurance just by filling out a form.

- Don't provide bank, credit card, personal information, or payment to someone who calls or comes to your door regarding ACA coverage. Assistance in navigating the Health Insurance Marketplace is available for free all over the country (go to HealthCare.gov and click "Find Local Help"), and real Marketplace representatives will not ask you for personal or financial data.

-Information provided by AARP

Home Repair Fraud

If you are a homeowner, it's not uncommon to have contractors show up on your doorstep uninvited. They typically say they were doing some work in the neighborhood and noticed that your house needed some repairs too. They'll offer to fix your roof, repave your driveway or perform other repairs or renovations, for what sounds like a great price. When that happens, be wary: The smiling fix-it man or woman at your door might turn out to be an unscrupulous contractor or an outright con artist, out to fleece you with a home improvement scam.

Shady contractors will often ask for payment up front. Some simply disappear with your money. Others will do shoddy work or claim to have discovered some hidden problem in your house that needs immediate attention and significantly raises the cost (a dishonest variation of the sales tactic known as upselling).

Con artists look to prey on homeowners when they are vulnerable. If your house has been damaged by a storm or natural disaster, a scammer may show up and try to persuade you to sign over the payment from your insurance company. Some crooks seek out older homeowners with memory or cognitive problems, hoping to con them into paying multiple times for the same work.

Here's what you can do to avoid being victimized by a home repair scam.

— Warning Signs —

- Beware of contractors who say they stopped by because they just happen to be in your neighborhood. The good ones are usually too busy to roam around in search of work.

- Be skeptical if a contractor says he can offer a lower price because he'll be using surplus material. That could mean he overbilled a previous customer or didn't finish the work.

Real Estate - Protect your Investment

- Foreclosure problems can sometimes be worked out, but you should start with your lender. Don't get involved in a Credit Restoration business until you have tried to help yourself. Companies who offer restoration assistance may charge fees and cannot guarantee that you won't lose your property in the end.

- You can report fraud or check the credentials of real estate professionals by contacting the California Department of Real Estate at 877-373-4542, or go online at www.dre.ca.gov.

Text Message Scams

Phishing is a fraudulent practice of sending scam emails. Scammers use phishing emails or text messages to trick someone into disclosing personal information, such as account numbers or Social Security numbers.

Never send any private information in a text message and never reply to a message asking you for personal information. Criminals may include the name of a legitimate company to lure you into thinking the text message is genuine. Call the company directly to inquire if the message is legitimate. Companies don't normally ask for a password or account number through text.

Never share your cell number on social media sites. Your cell phone number can be as valuable as your Social Security number in the wrong hands. Phony text messages can allow scammers to access your personal information including your email accounts.

Phony text messages often try to lure you into clicking on a link in the body of the message by offering you free gifts or prizes. Clicking on the link can install malware on your phone which collects data from your phone that is sold to others.

Place your cell number on the National Do Not Call Registry. Customers of AT&T, Sprint, or Verizon can report spam text messages by forwarding the message to 7726 (SPAM).

You can also make a report with the FTC at www.ftc.gov for any unsolicited text messages you receive.

Real Estate - Protect your Investment

The subject of Real Estate Fraud is too complicated to tackle in one page and not all problems are caused by outright fraud. There are unethical business practices and just plain “bad advice” that can do just as much harm as actual fraud. Your equity may be your biggest asset and your nest egg for your last years, so do not put something that precious into the hands of a stranger. Savvy consumers have been taken advantage of, so if it can happen to them, it could happen to you. If you discover something amiss in a Real Estate transaction seek help right away. Don’t sign until you check the credentials of a real estate professional or attorney.

Self-Defense Tips:

- Do not enter into any Real Estate agreement because of a phone call. Hang up and do your own research. If you don’t quite understand what you are doing, or you have not researched it enough, do not take a “leap of faith.” Don’t let embarrassment prevent you from talking to professionals about your needs and your plans before you sign something.

- If you have questions about your home equity or loan, talk to someone local. Your hometown banker, real estate professional, or your attorney will be able to advise you. A local business has a vested interest in you and a stronger desire to preserve their own reputation in their dealings with you. You will also have the benefit of meeting face to face, as well as home delivery or local pick up of paperwork to facilitate answers to questions before you sign.

- Don’t agree to become Joint Tenants with a family member, caregiver, or friend as a quick fix for Estate Planning because situations can change. Becoming Joint Tenants with a family member or any other person means that person has equal say in disposition of property. Making someone a joint tenant will cause you to lose your power to decide what you want to do with your property and when.

- A Quitclaim Deed is often used in financial elder abuse so don’t Quitclaim your property to family or others unless you get your own legal advice. A quitclaim is not reversible just because you change your mind. Never agree to quitclaim your property in exchange for lifetime care. Many seniors have been evicted from their own homes because they have quitclaimed their property to the wrong person.

Home Repair Fraud

— DOs —

- Do verify the license with the Contractor’s State License Board (CSLB). Check for status, scope of work approved under the license and the names of the workers under that license.

- Do insist on seeing references. The Federal Trade Commission (FTC) recommends asking past customers detailed questions, including whether the project was completed on time and if there were unexpected costs. The FTC also suggests asking the contractor if you can visit a job currently in progress.

- Do require a bid in writing and compare at least three bids from multiple contractors before agreeing to any work.

- Do get a written contract before you pay any money and before the work starts.

- Do read the fine print.

— DON’Ts —

- Don’t pay cash. The Federal trade Commission (FTC) recommends using a check or credit card or arranging financing.

- Don’t put down a big deposit. The contractor can only ask for 10% or $1,000, whichever is less, up front.

- Don’t automatically take the lowest bid. Some contractors cut corners to come in lower than competitors, according to the Better Business Bureau (BBB). The FTC recommends that if one contractor’s estimate is significantly less than those of competitors, ask why.

- Don’t let the contractor arrange financing for you. The FTC warns that you might be tricked into signing up for a home-equity loan with hefty fees or a high interest rate, or one in which the lender pays the contractor directly, giving him or her little incentive to finish the job or do it properly.

Identity Theft

Identity theft (ID theft) is the appropriation of personal information without your knowledge or consent, in order to commit fraud or theft.

How does ID Theft happen?

- Thieves steal your wallet, purse, luggage containing IDs, credit cards or other personal information.
- Thieves steal your mail, or dumpster dive in your trash cans.
- Thieves use the internet to obtain your personal information.
- Thieves use your personal information to obtain credit, insurance claims, employment, citizenship, Social Security, etc.

How can you decrease your risk of ID Theft?

- Reconcile your bank accounts monthly or more
- Review your free credit reports
- Shred sensitive papers before discarding, including receipts, catalogs and prescription bottles; they also have account information
- Guard your Social Security number. Do not carry your SS card with you!
- Carry only the credit cards you need that day
- Use a password other than your mother's maiden name

If your IDENTITY is stolen what do you do?

- Place fraud alerts with the three major U.S. credit reporting agencies (CRAs), also commonly known as the credit bureaus.
- Request copies of your credit reports from the three CRAs.
- Place a security freeze on your credit report.
- Obtain documents related to fraudulent transactions or accounts opened using your personal information.
- Obtain information from debt collectors.
- File a report with your local law enforcement agency.

Phony Collections Scams

Self-Defense Tips:

- Don't panic.- Understand that debt collectors have no legal authority over you, except through the court, and are governed by the Fair Debt Collection Practices Act.
- Demand to receive the debt information in writing within five (5) days of a collection phone call. If the collection agency refuses to supply you with written verification of the debt and the date the debt was incurred, they have broken the law, or it is a scam.
- Be aware that in California there are statutes of limitations on old debts.
- Understand that you have the right to provide a written request for no further contact from a collector and they must comply. Also, collection callers can only contact you between 8:00 a.m. and 9:00 p.m.
- Don't wire money at someone else's request-ever!
- Legitimate debt collectors will not take payments with gift cards.
- Don't give anyone your employment information, account numbers, social security number, or permission to debit your bank accounts, no matter how threating the phone calls become. An illegitimate collector may steal your identity.
- Don't believe threats that you will go to jail. People go to jail for fraud, not debt!
- Don't believe threats that you will be sued. You can report illegal debt collection practices to the Federal Trade Commission at 877-382-4357 www.ftc.gov, or the California Department of Consumer Affairs at 800-952-5210 www.dca.ca.gov.

Phony Spoof Scams

Scammers are using a variety of tactics to get victims to fall for scams. Phone spoofing is a method used to get victims to answer the phone. Scammers falsify the caller ID to make it seem as if a local number or a government agency is calling. Don't trust your caller ID; it may be a scam.

If you get an unknown call:

- Let it go to voicemail and check your voicemail to make sure it wasn't an important call.
- Remember, government agencies like the IRS will not call you.
- Don't give out any personal information.
- Don't wire money or send money via gift cards.

The C.A.R.E Program will help you determine the validity of the collector's demands and your rights under the law. Call APS at 800-491-7123

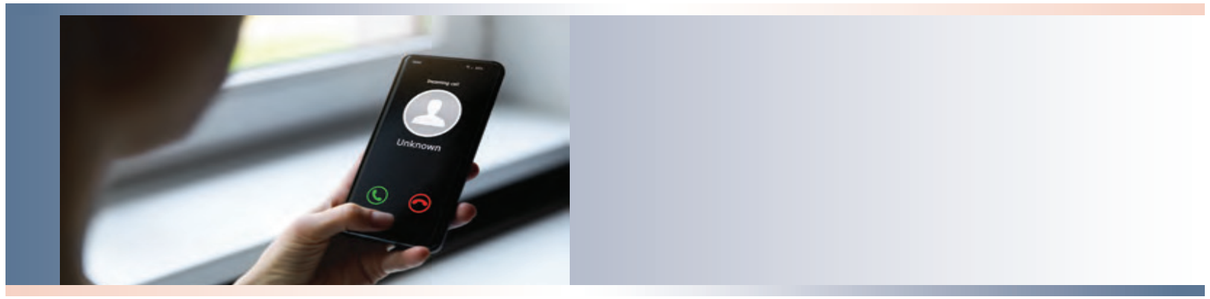
Phony Collections Scams

Phony bill collectors are calling consumers demanding immediate payment on non-existent debts, threating dire consequences if payments aren't made. Most often it is required that the money be wired, and if there is resistance, often a "discount" payment is offered. These aggressive, persistent calls at all hours are a scam, designed to scare people into paying money they don't owe. Even if you have existing debt, legitimate creditors do not conduct business this way. The C.A.R.E Program (800-491-7123) will help you determine the validity of the collector's demands and your rights under the law.

IRS Scam

Have you ever received a call from the "Internal Revenue Service (IRS)" stating you owe money? Hang up, this is a scam! Scammers impersonate the IRS stating there will be a consequence if you don't pay immediately. Scammers ask for gift cards, personal information, or money to be wired. Why do scammers want gift cards? As soon as the victim gives the scammer the pin on the back of the gift card, that money is gone and almost impossible to trace. The IRS will never call or email you asking for an immediate payment or personal information; they will mail you a notice. If you are unsure if you owe money to the IRS, call the IRS directly at 800-829-1040 or you can check online at IRS.Gov.

The Department of Treasury's Inspector General for Tax Administration (TIGTA) Unit is actively investigating these cases for the IRS. The TIGTA Agents (who are real Federal Agents) meet with the victims to get details on their case. For additional information go to: http://www.treasury.gov/tigta/contact_report_scam.shtml



Jury Duty Scam

A scammer calls identifying him or herself as being a government official accusing you of failing to comply with Jury Duty. Consequently, there is now a warrant for your arrest. In order for you to avoid arrest and jail time you will now have to pay a fine immediately. If you receive a call similar to this, hang up! This is not a real government official calling you. Scammers can manipulate caller ID information to make it appear as if a local number is calling. Scammers also use credible government titles to scare victims. They ask for prepaid gift cards or personal information that can be used for identity theft. Federal Court will contact you through U.S mail and would not ask for sensitive information via a telephone call.

Lottery and Sweepstakes Scams

Scam operators — often based outside of the US — are using the telephone and direct mail to entice U.S. consumers to buy chances in high-stakes foreign lotteries, from as far away as Australia and Europe. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

Still, federal law enforcement authorities are intercepting and destroying millions of foreign lottery mailings sent or delivered by the truckload into the U.S. Unfortunately, consumers, lured by prospects of instant wealth, are responding to the solicitations that do get through — to the tune of $120 million a year, according to the U.S. Postal Inspection Service.

The Federal Trade Commission (FTC), the nation's consumer protection agency, says most promotions for foreign lotteries are likely to be phony. Many scam operators don't even buy the promised lottery tickets. Others buy some tickets but keep the "winnings" for themselves. In addition, lottery hustlers use victims' bank account numbers to make unauthorized withdrawals or their credit card numbers to run up additional charges.

The FTC has these words of caution for consumers who are thinking about responding to a foreign lottery:

Phishing Email and Text Scams

Learn how to detect and report suspicious email and text messages, also known as 'SMS phishing' or 'smishing', that appear to be from your bank or creditor. If you receive a suspicious email or text message, don't respond, click on any links, or open attachments.

If you responded:

If you clicked on a link, opened an attachment, or provided personal or financial information, call your bank immediately and report it.

If you didn't respond:

Forward the suspicious email or send an email with the text message copy to your bank.

For your security, banks may contact you by email, text, or phone regarding your card or account activity. Only use their secure methods of communication to receive updates on demand.

When your bank contacts you, they will not ask for your card PIN, access code, or your online banking password. If you are uncomfortable about a request for information, do not respond and instead call the number on the back of your bank card to verify the authenticity of the request.

What is Phishing?

Phishing is usually a two-part scam involving an email or text message containing links to a fraudulent website requesting sensitive information such as username, password, and account details. Once obtained, your personal and financial information can be used to access your account and steal money.

How to recognize a phishing email

Phishing emails are becoming more sophisticated and difficult to distinguish from legitimate emails. By impersonating a reputable company's communications, these emails tend to use clever and compelling language, such as an urgent need for you to update your information or communicate with you for your security. To spot a phishing email, look for a combination of red flags.

Online Dating Scams

More people use dating websites and mobile apps every day. Although online dating may be a great way to socialize and build new relationships, it is also rampant with scammers looking to take advantage of unsuspecting people. Before using a dating website, be aware of the following tips to stay safe online.

- Use a dating site with a good reputation: Research the website before you join. Do a web search with the name of the site and the word “scam.”

- Avoid people who quickly request to leave the dating website and speak with you through email or instant messaging.

- Never disclose any personal information including your social security number, bank account number, address, or the names of your family members.

- Be cautious when speaking with someone online who states they are stranded in another country or need financial help. If someone asks for money, even if it’s to come and meet you in person, report them to the dating site and block them from contacting you. It’s never wise to give money to someone you don’t know.

- When speaking online or through email, be cautious of someone whose messages contain grammar or spelling errors. Look out for broken English or unusual word choices.

- If you do meet in person with someone you met online, meet in a public place. Also, tell someone you trust where you are going and with whom; ask them to check in with you periodically by text or phone while you’re out.

Never disclose any personal information including your social security number, bank account number, address, or the names of your family members.

Lottery and Sweepstakes Scams

- If you play a foreign lottery — through the mail or over the telephone — you’re violating federal law.

- There are no secret systems for winning foreign lotteries. Your chances of winning more than the cost of your tickets are slim to none.

- If you purchase one foreign lottery ticket, expect many more bogus offers for lottery or investment “opportunities.” Your name will be placed on “sucker lists” that fraudulent telemarketers buy and sell.

- Keep your credit card and bank account numbers to yourself. Scam artists often ask for them during an unsolicited sales pitch.

- The bottom line, according to the FTC: Ignore all mail and phone solicitations for foreign lottery promotions. If you receive what looks like lottery material from a foreign country, give it to your local postmaster.

— Red Flags —

- You receive notice you have “won” when you don’t recall purchasing a ticket
- You must act now
- You can’t tell anyone
- You are required to pay some sort of fee for your so-called, winnings
- You are instructed to pay fees with prepaid cards (iTunes, Green Dot, etc.)

Oftentimes, victims of lottery/sweepstakes scams receive a check or money wire and are instructed to send a portion of that money to pay for so-called, taxes, attorney fees, storage fees, etc. Then the check/wire is determined to be fraudulent. The banks will hold you responsible. This can result in not only the loss of the amount of the money withdrawn, but any fees associated with it.

If you are contacted by someone stating you have won, do not give them any money, bank account numbers, Social Security numbers or any other personal information. Report it to your local law enforcement and the Federal Bureau of Investigation (FBI) at www.IC3.gov

Medicare Drug Benefit Scams

You have probably seen at least one news article related to various prescription drug plan telemarketing schemes. As usual, the scammers have been busy figuring out new ways to steal your money!

The trick often involves a telemarketing call asking seniors for their social security number, personal bank account information and sometimes offering a new Medicare card for a fee. When the telemarketer receives the requested account information, an amount (usually under $400) is withdrawn electronically to pay for the illegitimate Medicare card or prescription drug plan. The callers may use fictitious or generic sounding business names such as National Medical Office, Medicare National Office, and National Medicare.

Self Defense Tips:

- Hang up if you receive a call requesting your Medicare number, social security number, bank account information or payment regarding your Medicare drug benefits. Legitimate Medicare drug plans will not ask you for payment over the phone or the Internet; it is against Medicare's rules. They must send you a bill for the monthly premium.
- If you have become a victim of this type of scam, or if you have questions about a drug plan, please call Medicare directly toll free at 1-800-Medicare (1-800-633-4227), TTY 1-877-486-2048, or visit Medicare.gov.

Hang up if you receive a call requesting your Medicare number, social security number, bank account information or payment regarding your Medicare drug benefits.

Money Mule Scams

A money mule is a person who receives money, that has been acquired illegally, and sends or transfers the money on behalf of another person. Money mules often are not aware that they have been targeted by a scammer and are unaware that they may be participating in money laundering. A person that is a knowing money mule and is receiving a portion of the money to send to another person is actively participating in money laundering.

How does a person typically get involved as a money mule?

- Romance scams
- Lottery scams
- Work-from-home scams

DO NOT BE A VICTIM.
DO NOT BECOME A PERPETRATOR.

What do these scams have in common?

The victims of these scams have all been tricked into giving the scammer money until they can no longer give the scammer money. The scammer then offers the victim the opportunity to "earn" back his/her money by receiving cash in the mail, allowing the use of his/her bank account, or depositing fraudulent checks into the bank account. Then the victim is allowed to keep a small portion of the money and is required to send the money to another potential money mule, which eventually gets to the scammer. The victim is now a knowing and active participant in money laundering.