FRAUD PREVENTION
SDPD Crime Prevention
October 6, 2017

CONTENTS

This paper contains tips for preventing telemarketing and other phone fraud, Internet fraud, and other scams. If you live in San Diego and lose money in any of these scams, report it to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Otherwise report it to your local law enforcement agency. Links to additional tips on cybersecurity, identity theft prevention, and cybersecurity for businesses are on the prevention tips page of the SDPD website at **ww.sandiego.gov/police/services/prevention/tips**.

TELEMARKETING AND OTHER PHONE FRAUD

Callers claiming to represent everyone from police officers to the disabled take advantage of the public's sympathy and generosity to the tune of billions of dollars each year. They also offer miracle cures for everything from baldness to cancer, vacation time shares, sweepstakes prizes, chances to earn enormous profits from no-risk, high-yield business and investment opportunities, etc. You can be sure it's a scam if they ask for money or personal information, especially if they use scare tactics. And you should be suspicious of all solicitors. Here are some examples of phone scam calls.

- You've won a prize or lottery and that you need to send money first or provide bank account information to get your winnings.
- You've won a gift card at a local store and have to come in a pick it up right away. When you leave your home it is burglarized. Call the store to verify the prize. And make sure your home is secure whenever you leave it.
- You have to act right away. Remember, if it's a good deal today it will still be a good deal tomorrow. Don't let anyone rush you into signing anything.
- He or she is calling on behalf of a charity that has a variation of an official or nationally-recognized name, e.g., Salvation League instead of Salvation Army.
- He or she is a law enforcement officer and threatens to arrest you if you don't pay a fine for a bogus charge, e.g., a speeding violation caught on a camera or a failure to appear for jury duty. Payments are usually requested by prepaid debit card or money order. The scammer might also use the name of a real officer, use some of your personal information that can be obtained on the Internet, and make the department's phone number appear on your Caller ID, all to make the call convincing. No law enforcement employee will ever contact you to demand money or any other form of payment. Hang up immediately if you get this kind of call.
  If you think you may have missed jury duty, you can call the Superior Court at **(619) 450-5757** and press 0 to talk to a person. If you are threatened about an outstanding warrant you can go to **www.sdsheriff.net/courts** to see if there is one outstanding.
- You need to attend a sales meeting to take advantage of this limited offer.
- You need to dial a pay-per-call **900** number.
- You need to call a number in a strange area code, e.g., **876** which in Jamaica. In addition to soliciting money and personal information, these calls can be expensive with the cost being split between the phone company and the number owner. So the longer you talk, the more money the number owner gets. So never call back a number with an area code you don't recognize. You can get area-code locations online, e.g., at **www.areacodelocations.info/areacodelist.html**.
- He or she is calling from the security or fraud department of your credit- or debit-card company and asks you for the 3-digit security number on the back of your credit card to verify your possession of the card to aid it in a fraud investigation.
- Medicare now requires a National ID Card and offers to provide one for a fee. Or the caller says a card is being mailed but he needs your bank information. Call the Health Insurance Counseling and Advocacy Program (HICAP) at **(800) 434-0222** to report any solicitations regarding Medicare.
- He or she is a U.S. Food and Drug Administration (FDA) agent or official and that you must pay a fine because you have bought or attempted to buy discounted prescription drugs from a foreign pharmacy. Report such calls to the FDA Office of Criminal Investigations at **(800) 521-5783**.
- He or she is calling from Microsoft or some legitimate company to warn you that your computer has a security problem and offers a free security check. You may then be tricked into buying some software or services that you don't need, giving out credit card information, and allowing access to your computer so malware can be downloaded. If you fall for this scam you should change your computer and financial institution passwords, scan your computer for malware, and contact you bank and credit card providers.
- He or she is calling from the San Diego County Registrar of Voters and asks for your Social Security Number (SSN) to confirm that you are registered.
- He or she is calling from the Social Security Administration (SSA) and offers to help you apply for disability benefits. The scammers will try to get you to give or confirm your SSN. You can tell it's a scam because

SSA representatives will not make unsolicited calls and request personal information. If you have questions about disability benefits, or get calls offering help with them, call the SSA **(800) 772-1213**. You should also report the fraud attempt to the SSA Office of the Inspector General at **https://oig.ssa.gov/report**.

- You need to call an unfamiliar phone number because you are the respondent in a lawsuit and have 48 hours to respond. The caller also says that a restraining order had been issued as part of the proceeding. Don't call the number. Google it to see if it is a legitimate business or the source of threatening phone calls. In the former, the most likely search result would be the website of the business or possibly a website describing that business. In the latter, you might find websites where individuals post harassing, threatening and scamming phone calls that they receive. While the results may not be definitive, you will likely get some idea as to the legitimacy of the source.
- He or she is calling to enroll you in a health insurance plan under the Affordable Care Act (ACA), commonly called Obamacare, or to sell you an insurance card that is "required" to obtain the insurance. Nobody from the federal or state government will contact you about this, much less ask you to wire money, load money onto a prepaid debit card, or provide your bank account routing number or any other personal information. Hang up on any of these callers. And don't press any key to talk to an operator or get your name taken off their list. Visit **www.HealthCare.gov** if you want information about health insurance in your state.
- He or she is from San Diego Gas & Electric (SDG&E), says that you are late on a payment and if you don't pay immediately your gas and electricity will be cut off. You are told to buy a prepaid debit card and call back with its number. SDG&E says it does not contact customers by phone and ask for credit card information. Furthermore, under rules mandated by the California Public Utilities Commission (PUC), power companies must tell customers who are behind on their payments that they can set up a bill-payment plan giving them at least three months to get accounts up to date. Call SDG&E at **(800) 411-7343** if you have any concerns about being contacted or have any billing-related questions.
- He or she is from the Department of Motor Vehicles (DMV) and threatens to suspend your driver license if you don't pay your registration fee now.
- He or she is calling to sell magazine subscriptions, especially if special promotional offers are involved.
- You are eligible to receive a free medical-alert device purchased by a friend or relative. All you have to do is provide your credit card information so you can be billed for the service charges.
- You owe taxes and must pay using a pre-paid debit card or wire transfer. See the later section on IRS scams for more information on them.
- After the Equifax breach was announced in September 2017 you get a call saying "This is Equifax calling to verify your account information." This is a scam. Don't say anything and hang up. Equifax will not call out of the blue trying to trick you into giving personal or financial information.

Hang up immediately if the caller is rude or threatening. If you live in San Diego and receive repeated harassing calls, or calls in which you are threatened with physical harm and think the treat is real, report them to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Otherwise report it to your local law enforcement agency.

If you fall for one of these pitches, you may find:

- You never receive any "winnings" from the lottery you entered.
- The merchandise you bought is overpriced and of poor quality.
- The "free gift" never arrives, or if it does it's not worth the "shipping and handling" fee you paid.
- The investment turns out to be nonexistent or a loser.
- The donation you thought was going to a charity goes instead into the fundraiser's pocket.
- Unauthorized charges start appearing on your credit card statements.
- Con artists call and offer to help you get your money back, for a fee of course.
- Your computer has been infected with malware and ransomware.

The following tips will help you avoid and resist these scams.

- Never give your credit or debit card, checking account, Social Security or Medicare number, or any personal information to an unknown caller. Just hang up on anyone who asks for money, especially by a wire transfer, personal or financial information, or threatens legal action, e.g., a call from someone who says he's from the IRS, which never calls about a tax debt without first sending you a bill. More on IRS impersonation scams is covered in a later section.
- Don't ever assume a friendly voice belongs to a friend.
- Hang up on anyone who asks a simple question when you pick up the phone, especially if the answer is "yes." For example, if the question is "can you hear me?" and you say "yes," the scammer will record your voice and use it to verify your agreement to buy something expensive. Then if you complain you're warned that the recording is essentially a contract and that legal action will be taken against you if you don't pay.
- Ask the caller who they are and why are they calling if they ask for you by name. This puts the caller on the defensive and disrupts the script for their call.
- Hang up if you pick up the phone and say "hello" only to hear silence on the other end. This happens sometime with telemarketers who wait until a person comes on the line before speaking.
- Take the caller's name and phone number and say you'll call back if the caller says he's from a place you have an account or do business with. However, don't call that number. Look up the phone number or use the one you have and call it. You might find that no one with the caller's name works there and there's no problem with your account.
- Install Caller ID on your phone and be on guard when you see a number you don't recognize or a call classified as "private" or "unknown." In any case, you can't rely on the number shown. Scammers can hide their identities with a spoofing device that causes a fake number to appear on the Caller ID window. Under the Federal Truth in Calling Act, Federal Communications Commission (FCC) rules prohibit any person or entity from transmitting misleading or inaccurate Caller ID information *with the intent to defraud, cause harm, or wrongly obtain anything of value.* If no harm is intended or caused, spoofing is not illegal. Anyone who is illegally spoofing can face penalties of up to $10,000 for each violation. In some cases, spoofing can be permitted by courts for people who have legitimate reasons to hide their information, such as law enforcement agencies working on cases, victims of domestic abuse or doctors who wish to discuss private medical matters. You should file a complaint with the FCC if you suspect illegal spoofing. The number of the Consumer Help Center is **(888) 225-5322**. More information on spoofing and Caller ID is available on the FCC website at **https://consumercomplaints.fcc.gov/hc/en-us/articles/202654304-Spoofing-and-Caller-ID**.
- It's better if you don't answer when you don't recognize the number. Then if the caller leaves a message, you can decide later whether to call back.
- Never give out the 3-digit security number on the back of your credit or debit card unless you have initiated a card purchase and the seller asks for it to verify your possession of the card.
- Ask a charity to send written information about its finances and programs before making any commitments.
- Call the Better Business Bureau (BBB) of San Diego, Orange, and Imperial Counties at **(858) 496-2131** to check on any unsolicited offers. Or visit its website at **www.bbb.org/sdoc** to see whether the business is accredited. And for any business you can check its rating, reason for the rating, the number of closed complaints in five categories, and since May 2012, detailed information on consumer complaints, the responses a business made to the complaint, and subsequent correspondence between the consumer, the business, and the BBB. (The names of consumers who complain will still be kept confidential.) The BBB's website also has general consumer information and tips on avoiding various types of fraud.
- For additional information on telemarketing and other phone scams see the Federal Trade Commission (FTC) website at **www.consumer.ftc.gov/articles/0076-phone-scams** regarding the signs of a phone scam, how they hook you, why they're calling you, how to handle an unexpected sales call, and what to do about pre-recorded (robo) calls.

To reduce pre-approved credit offers and telemarketing calls you should list your home and mobile phone numbers free on the National Do Not Call Registry (NDNCR). Call **(888) 382-1222** or register online at **www.donotcall.gov**. Law-abiding telemarketers check the registry every 31 days so it may take that long before your numbers are removed from their call lists and you can file a complaint. This should stop all but exempt calls from charities, political organizations, survey companies, and companies you have dealt with recently or signed a contract with that gives it permission to call you. If telemarketers ignore the fact that your numbers are on the registry you can file a complaint at the above number or website. For this you'll need to keep a record of their names and the dates of the calls.

If you receive non-exempt recorded solicitations known as robocalls, also banned by the FTC, you can file a complaint even if your number is not on the NDNCR. This can be done online at **www.ftc.gov** or by phone at **(877) 382-4357**. If your phone system has a feature called "simultaneous ring" it is now possible to stop non-exempt robocalls by subscribing to a free service at **www.nomorobo.com**. With simultaneous ring, the call first goes to a Nomorobo number where it's analyzed and terminated if it's not exempt. The call won't even ring on your phone. If you can't have these calls stopped there are several things you can do minimize their annoyance and keep from becoming a victim of telemarketing fraud. First, don't answer calls from unfamiliar numbers. If you do answer and you hear a recording, hang up immediately. And if you don't hang up, never press any numbers for information or to be put on the NDNCR. You should also file a complaint with the FTC. Also, ask your phone service provider if it offers a robocall blocking service. If not, encourage your provider to offer one. You can also visit the FCC's website at **www.fcc.gov/unwanted-calls** for information and resources on available robocall blocking tools to help reduce unwanted calls.

Under its amended Telemarketing Sales Rule (TSR) dated June 13, 2016, the FTC has made it illegal for telemarketers to ask people to pay with systems that deliver a quick, anonymous cash payout with cash-to-cash money transfers like those from MoneyGram, and PINs from cash reload cards like MoneyPak. The amended Rule bans telemarketers from asking for your bank account information and using it to create a remotely-created check that you never see or sign. It also requires the disclosure of certain information and prohibits misrepresentation, calls to consumers outside of 8 a.m. to 9 p.m., abandoned outbound calls subject to a safe harbor, unauthorized billing, and other fraudulent activities. A guide for telemarketers in complying with the amended TSR is online at **www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule#callingtime**.

Some wireless providers now have a free service that warns its subscribers if an incoming call appears to be from a scammer. When this happens, it will display "Scam Likely" on the phone's Caller ID. In a companion service, calls from known scammers will be blocked from ringing a subscriber's phone. Because there's a chance that calls from legitimate numbers would be blocked, subscribers will have to opt for this service. Check about with your provider about these services. They can save you a lot of time a money.

INTERNET FRAUD

In 2016 the FBI's Internet Crime Complaint Center (IC3) received 298,728 complaints on its website reporting total dollar losses of over $1.3 billion. Many of these are referred to law enforcement agencies for further consideration. You may be at risk if you answer "yes" to any of the following questions:

- Do you visit websites by clicking on links within an e-mail?
- Do you reply to e-mails from persons or businesses you are not familiar with?
- Have you received packages to hold or ship to someone you met on the Internet?
- Have you been asked to cash checks and wire funds to someone you met on the Internet?
- Would you cash checks or money orders received through an Internet transaction without first confirming their legitimacy?
- Would you provide your personal banking information in response to an e-mail notification?

If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the IC3 at **www.ic3.gov**. Its website also includes press releases on the latest scams and other Internet dangers, and tips to assist you avoiding a variety of Internet frauds. You should also contact your e-mail provider. Most keep track of scams. Send your provider the suspicious message header and complete text. For more information on Internet fraud, visit **www.LooksTooGoodToBeTrue.com**.

The following material deals with e-mail scams and online shopping frauds. Other scams involving the Internet and e-mail are described in the next section along with tips on recognizing and avoiding them.

E-mail Scams

Cybercriminals use e-mail in many clever ways to try to take your money and identity, and disrupt your computer operation, gather sensitive information, or gain unauthorized access to your computer. To protect your assets and computer you should never reply, click on any links, or open any attachments of e-mails that offer great bargains. If you want to click on a link, check the Uniform Resource Locator (URL) first by hovering over it, not clicking, to see if the destination name matches the URL exactly. If it doesn't, it's a scam designed to take you to a fake website. And if you don't recognize the sender, you should delete the e-mail without even opening it. Be especially suspicious about the following:

- Business opportunities to make money with little effort or cash outlay
- Offers to sell lists of e-mail addresses or software
- Any offer that asks for immediate action
- Chain letters involving money
- Work-at-home schemes
- Health and diet claims of scientific breakthroughs, miraculous cures, etc.
- Get-rich-quick schemes
- Free goods offered to fee-paying group members
- Investments promising high rates of return with no risk
- Kits to unscramble cable TV signals
- Guaranteed loans or credit on easy terms
- Credit repair schemes
- Vacation prize promotions
- Renew magazine or newspaper subscriptions
- Special offers that require a credit check and a small fee for verification expenses to be paid by a credit or debit card
- Free offer to remove ransomware from your computer
- Notices of prize or lottery winnings that require you to pay a fee to cover expenses
- Offers to enroll you in a health insurance plan under the ACA, commonly called Obamacare
- Requests for personal or financial information

Regarding the latter, cybercriminals often pose as government agencies or financial institutions that you normally deal with. Remember that government agencies never send important things by e-mail, and your financial institutions already have your personal information. If you suspect something might be a scam, check it out on Hoaxslayer at **www.hoax-slayer.com**. This website is devoted to debunking e-mail hoaxes and exposing Internet scams. It is constantly increasing its compiled list of scams. Regarding chain letters, The Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) recommends being especially cautious if the e-mail has any of the following characteristics:

- Suggests tragic consequences for not performing some action
- Promises money or gift certificates for performing some action
- Offers instructions or attachments claiming to protect you from a virus that is undetected by anti-virus software
- Claims it's not a hoax

- Includes multiple spelling or grammatical errors, or the logic is contradictory
- Urges you to forward the message

If an e-mail looks suspicious, it is always best to err on the side of caution and delete the message or mark it as junk mail. And as always, think before you act and be wary of any communication that asks you to act immediately, requests personal information, or just sounds too good to be true.

Online Shopping Frauds

If you use a credit card the federal Truth in Lending Act limits your liability to $50 for any unauthorized or fraudulent charges made before you report the billing error. To protect yourself you need to write to your credit card company within 60 days after the date of the statement with the error and tell it: (1) your name and account number, (2) that your bill contains an error and why it is wrong, and (3) the date and amount of the error. You need to pay all other charges but not the disputed amounts.

Don't use a bank debit card when shopping online, especially on an unfamiliar website. If something goes wrong your account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills. The federal Electronic Funds Transfer Act provides some liability protection in the event of any fraudulent charges resulting from the loss or theft of your card, or your card data. In the latter case you would not be liable for any fraud charges if you report them within 60 days after you receive your bank statement. But even then your bank is not obligated to restore your funds for at least two weeks while it investigates. But if you fail to report the fraud charges within 60 days of receiving your bank statement there is no limit on your liability. So if have to use a debit card, use one that is reloadable. Then you only risk the amount you put on the card if something goes wrong.

Consumers should be aware that if a deal looks too good to be true, it probably is. In one scam the victim located a car on the Auto Trader website and contacted the seller directly by e-mail. He was told that the car would be shipped to him for inspection and approval if he wired the money to a bank account where it would be held in escrow. He wired the money but the car never arrived. To prevent this kind of scam consumers need to be diligent in verifying all the parties involved in the purchase by phone calls, face-to-face meetings, etc. In a similar case the consumer asked to see the car before wiring any money. The scammer ended all contacts at that point.

Online scams also promise great deals on rental housing, airline tickets, concert tickets, timeshare properties, and vacation packages. The biggest red flag is when payment is requested by a wire transfer. It's difficult to track these transfers and almost impossible to get a refund. Check out the company offering the deal before making a purchase. Deal only with reputable sellers. Read the fine print and make sure you understand the terms, conditions, and refund/exchange policy of the sale. If it and the deal appear to be legitimate, pay by credit card and not by wire. Then if the deal turns out to be fraudulent, you can dispute the charges as indicated above.

OTHER SCAMS

This section contains tips on recognizing and avoiding the scams listed alphabetically in the Contents.

Information on preventing these and many other scams is available at no cost from the California Department of Consumer Affairs. A complete list of its publications is online at **www.dca.ca.gov/ publications/index**. They can be viewed online or ordered by calling **(866) 320-8652**. Additional information about protecting yourself from fraud and identity theft is available on **www.STOPFRAUD.gov**, the website of the Federal Financial Fraud Enforcement Task Force established in 2009 to improve federal and state government efforts to investigate and prosecute significant financial crimes, and to recover their victim's losses. Other agencies that publish a great deal of information about scams and their prevention are the FTC at **www.ftc.gov** and the IRS at **www.irs.gov**, and the FCC at **www.fcc.gov**.

Also, any San Diego resident over the age of 60 can obtain free legal advice on recouping money lost to scams by calling Elder Law & Advocacy at **(858) 565-1392**. This state- and county-funded nonprofit corporation provides no-cost routine legal services to seniors and caregivers of seniors.

Additional Veterans Benefits

In this scam unscrupulous investment sales agents promise older veterans that they can get them additional benefits by overhauling their investments. This usually involves the transfer of a veterans retirement assets to an irrevocable trust to make the family appear impoverished so the veteran can qualify for a pension and related programs that pay additional benefits for everyday living expenses. The investments are either completely bogus, in which case the veteran loses all his or her assets, inappropriate for older retirees, or ones that generate a high commission for the agent. While the Veterans Administration (VA) does not examine veterans asset histories for determining pension eligibility, Medicaid does and its benefits can be jeopardized by such asset transfers. Veterans can avoid this scam by doing the following:

- Don't be fooled by agents who say they represent official-sounding veterans organizations.
- Be wary of sales pitches made at free-meal seminars sponsored by nursing homes, community centers, assisted-living facilities, etc. They often receive a fee to let sales people make so-called educational presentations. (See the section on high-pressure sales of financial products at free-meal seminars above.)
- Contact the California Department of Veterans Affairs at **(800) 952-5626** for official information about veterans benefits. Or see an overview of the benefits administered by the Department at **www.calvet.ca.gov/veteran-services-benefits**.
- Contact the California Department of Business Oversight (DBO) at **(866) 275-2677** to find out if the sales agent is licensed. Or get license information directly at **http://search.dre.ca.gov/integrationaspcode/**.

Veterans should also avoid dealing with companies that offer cash in exchange for an assignment of future benefit and pension payments. While these pension buyouts and quick-cash loans are not necessarily illegal, the U.S. Department of Veterans Affairs calls these offers "financial scams" that take advantage of desperate veterans who may be down on their luck and need quick cash. The buyouts typically pay only a fraction of a veteran's actual entitlement over time, about 30 to 40 cents on the dollar. And on loans, interest rates may exceed 30 percent.

Appeals for Help

This scam usually involves a call for help from a person claiming to be a family member, e.g., a grandson, who says he's been arrested or hospitalized in a foreign country and needs cash quickly in the form of a money-wire transfer but is afraid to call his parents. Grandparents are often targeted. Scammers get the names of family members from obituaries or social networking sites on the Internet. They also use these sites to learn about foreign travel by family members. You can protect yourself from these appeals by doing the following:

- Listen to the caller and take notes, including the person's caller ID.
- If a caller says he's your grandson, ask which one. But don't provide a name. Most scammers will hang up.
- Ask a question that only your grandson would be able to answer correctly.
- Confirm your grandson's location and identity by saying you will return his call at his home or on his cell phone, but don't ask for the numbers. Get them from a trusted family member.
- If the call involves an arrest, contact the U.S. Embassy in the country involved and ask for assistance and verification of the arrest.
- Never provide bank account, credit-card, or debit-card numbers to any caller.
- Be very suspicious of any requests for money wires.
- Report the scam to the SDPD or the FBI. Scams coming from Canada can be reported on **www.antifraudcentre.ca**.

A variant of this is called the Red Cross scam. It preys on the family of military personnel deployed overseas. The scammer claims to be with the Red Cross and says that their loved one has been injured. They then ask for your SSN to authorize help. They might also ask for money up front. Family members should clear any injury report through the appropriate chain of command or contact the base family community services for help. They should never give out any personal information or send money.

Auto Loan Modification

If you're having trouble paying your car loan and you're worried about having your vehicle repossessed, you may think about doing business with a company that claims it can reduce your monthly car loan or lease payment and help you avoid repossession. These companies might charge fees of several hundred dollars up front, tout their relationships with lenders, and bolster their claims to be able to significantly lower your monthly payments with glowing testimonials from "satisfied" customers. Some say that if they can't make a deal with your lender, they'll refund your money.

These promises sound like a way to solve your problem. But the FTC says they're just smooth talk by scam artists who are out to take your money and provide nothing in return. Many never even contact the lenders. The scam artists often compounded the problem by telling their clients to stop making their car payments while the companies claimed to be in negotiations with lenders. Some victims learned that nothing had been done anything only after their lender contacted them about repossessing their vehicle.

If you are having trouble making car payments contact your lender directly to discuss your options as early as you can. The longer you wait to call, the fewer options you will have. Typical auto loan modifications involve either deferring missed payments to the end of the loan or extending the loan term to reduce monthly payments. That choice actually increases the total amount you pay in interest, even with a lower interest rate. Lenders rarely reduce the amount of the principal or the interest rate in an auto loan modification.

Bankruptcy Foreclosure Rescue

Bankruptcy foreclosure scams target people whose home mortgages are in trouble. Scam operators advertise on the Internet and in local publications, distribute flyers, or contact people whose homes are listed in foreclosure notices. They may promise to take care of your problems with your mortgage lender or to obtain refinancing for you. Sometimes they ask you to stop making your mortgage payments or make the payments to them. But instead of contacting your lender or refinancing your loan they pocket the money you paid and then file a bankruptcy petition or a predatory lending lawsuit in your name, often without your knowledge. If this happens you could also lose your home. So proceed with care in dealing with any individual, company, or law firm that does any of the following:

- Makes an unsolicited contact and uses high-pressure sales techniques
- Calls itself a mortgage or foreclosure consultant, foreclosure prevention specialist, or any similar title
- Says it knows a lot of people who have gone through foreclosure and just wants to help you
- Contacts you because they saw a notice of default or a notice of trustee's sale of your home in public records
- Promises to find "loopholes" in your loan documents or violations of State or Federal lending laws that can get you off the hook
- Asks for a fee before performing a service
- Asks you to make your home mortgage payments directly to them
- Asks you transfer you property deed or title to them.
- Sends you a mailer promising mortgage relief via a lawsuit against banks and lenders, and asks for an up-front fee to join a mortgage fraud lawsuit against banks and lenders that would help you avoid foreclosure, get rid of your mortgage, or help you get money from your lenders.

- Uses Spanish-speaking salespeople with a Spanish-language script to help establish credibility and make their targets feel more comfortable.

Here are some ways to avoid becoming a victim of a mortgage foreclosure scam.

- Read the brochure entitled *Fraud Warnings for Homeowners in Financial Distress* published by the California Bureau of Real Estate (CalBRE) in the Department of Consumer Affairs. It's online at **www.calbre.ca.gov/files/pdf/FraudBrochure0909.pdf**.
- Don't transfer ownership of your home to anyone who promises to save it. Sometimes scammers will say they can negotiate directly with your mortgagor to keep you in your home on terms you can afford. They might ask you to execute a financial power of attorney for their benefit in order to assist them in negotiating on your behalf. After some period of "negotiating" they will tell you they've put together a great deal through which you can avoid foreclosure. Almost always some part of this deal will involve granting the scammer ownership of your home. In another refinancing scam the terms will secretly be so oppressive that you have no hope of paying the new loan. You will most likely default and the scammer's company will end up with your home.
- Don't transfer ownership of your home to anyone who promises to sell your home and share the proceeds with you. In the most basic scams foreclosure consultants try to win your confidence and then ask you to sign a grant deed granting them sole ownership of your home. They promise to make the mortgage payments, delay the foreclosure, and then sell your home to pay off the mortgage and bring you a cash profit out of the proceeds. They will then somehow split the proceeds with you as compensation. In a more sophisticated version of this scam foreclosure consultants have you sign a detailed contract in which they promise to sell your home for you. A formal contract gives the transaction the appearance of trustworthiness and helps them try to avoid claims of fraud or other illegality. Ultimately, the contract requires you to grant them sole ownership of your property, and move out so they can sell it. They falsely promise to find you a new apartment, help you pay the rent, give you a small amount of cash up front, and then somehow share the proceeds with you.
- Don't transfer ownership of your home to anyone who promises take your home and rent it back to you. In this scam consultants tell you that your best option for avoiding foreclosure is to transfer ownership of your home to them and then have them rent it back to you. The consultants will most likely describe some kind of financing transaction where it buys out your mortgage or arranges some kind of refinancing for you.
- Don't deed your property to anyone you are not selling it to and who is not paying off your mortgage at the closing. And don't rely on a promise to lease the property back to you or let you buy it back in a few years.
- Don't pay advance loan-modification fees to anyone, including a licensed real estate broker or an attorney. Advance fees are now prohibited in California. It's illegal for a company to charge you a penny until it gives you the following: (1) a written offer for a loan modification or other relief from your lender, (2) a document from your lender showing the changes to your loan if you decide to accept its offer, (3) a document clearly showing the total fee it will charge you for its services, and (4) you accept the lender's offer.
- You can check a real estate broker's license at **www2.dre.ca.gov/PublicASP/pplinfo.asp**.
- Be careful in selecting an attorney. Don't rely on ads that claim the attorney is a member of the State Bar of California. All attorneys are members of the Bar and not all have special knowledge, experience, or expertise in loan modifications. In fact, it appears that many attorneys offering these services have little or no prior experience in loan modifications. You can check whether a person is a licensed attorney and see his or her membership record on the California Bar's website at **www.calbar.ca.gov**.
- Read all documents carefully before signing them. A scammer will often bring you a lot of documents to sign quickly as a part of the work he or she claims to be doing on your behalf. Eventually the scammer they will try to sneak a grant deed into these documents. If you sign it you will unknowingly sign away ownership of your home. If you knowingly sign a deed, make sure a notary you trust is present to notarize the document.

- Make sure the person who negotiates, attempts to negotiate, arranges, attempts to arrange, or otherwise offers to perform a mortgage loan modification or other form of mortgage loan forbearance for a fee or other compensation paid by the you, the borrower, provides the following to you in not less than 14-point bold type prior to entering into any fee agreement as required in California Civil Code (CC) Sec. 2944.6(a):

  "It is not necessary to pay a third party to arrange for a loan modification or other form of forbearance from your mortgage lender or servicer. You may call your lender directly to ask for a change in your loan terms. Nonprofit housing counseling agencies also offer these and other forms of borrower assistance free of charge. A list of nonprofit housing counseling agencies approved by the United States Department of Housing and Urban Development (HUD) is available from your local HUD office or by visiting **www.hud.gov**."

  This statement can be included in the contract or provided separately. And if the negotiations are conducted in Spanish, Chinese, Tagalog, Vietnamese, or Korean, a translated copy of this statement shall be provided to you as required in California CC Secs. 1632(b) and 2944.6(b). Go to **www.hud.gov/offices/hsg/sfh/hcc/fc** for a list of nonprofit housing counseling agencies approved by HUD. There isn't a local HUD office in San Diego.
- Don't make your mortgage payments to anyone other than your lender.
- Don't work with anyone who tells you not to contact your attorney, lender, or a credit or housing counselor.
- If you deal with a foreclosure consultant as defined in California CC Sec. 2945.1 who is not an attorney or a real estate broker, make sure that person has obtained a Certificate of Registration as a Mortgage Foreclosure Consultant from the California Department of Justice (DoJ). This is now required in California.
- Before hiring a consultant check the California Attorney General's website at **www.ag.ca.gov/loanmod** for tips to avoid being scammed and other information.

If you can't pay your mortgage, call your lender as soon as possible for help. You don't have to be in default to obtain a mortgage modification, as discussed below. The further behind you fall the more likely you are to lose your home. There are also many non-profit agencies that can help you with loan modification without a fee. You can get a list of housing counseling agencies approved by HUD by state and city on its website on the page entitled Foreclosure Avoidance Counseling at **www.hud.gov/offices/hsg/sfh/hcc/fc/**. As of February 8, 2017 there were 10 HUD-approved agencies in San Diego. Their counseling services are provided free of charge. One is Housing Opportunities Collaborative. Its phone number is **(619) 283-2200**. Its website is **www.housingcollaborative.org**. There is no need to pay a private company for these services. And remember, if you do engage a real estate broker or attorney, check on their licenses and only pay their fee after they have completed their work.

Suspected scams should be reported to the San Diego County District Attorney's Real Estate Fraud Program. Call its complaint line at **(619) 531-3552** to request a complaint form. Write or type a summary of your complaint and attach it to the complaint form. Your complaint cannot be reviewed without a complete concise statement of the facts. If bankruptcy proceedings are involved, call the United States Trustee at **(619) 557-5013**. The Trustee is a U.S. Justice Department official who monitors the bankruptcy system.

If you paid a licensed attorney for assistance in obtaining foreclosure relief and the attorney failed to perform legal services with competence, you should file a complaint with the State Bar by calling the Attorney Complaint Hotline at **(800) 843-9053** or by filing a written complaint. Information on filing a complaint and the complaint form are available on the State Bar website at **www.calbar.ca.gov**. The grounds for ethics violations in dealing with foreclosures can be found on the State Bar website by searching Ethics Alert and selecting the document entitled *Legal Services to Distressed Homeowners and …* Note that attorneys are prohibited from contacting you in person or by telephone based on a referral from a foreclosure consultant or someone else unless the attorney has a family or prior professional relationship with you.

In addition to these California remedies, consumers can file a complaint with the FTC by calling **(877) 382-4357** or going to **https://www.ftccomplaintassistant.gov/**. In its Mortgage Assistance Relief Services (MARS) Rule, the FTC is now banning mortgage relief companies from collecting advance fees and telling

consumers to stop communicating with their lenders or loan servicers. It is also requiring companies to disclose the following:

- They are not associated with the government, and their services have not been approved by the government or the consumer's lender or servicer.
- The amount of their fee.
- The lender may not agree to change the consumer's loan.
- Consumers may lose their home and damage their credit rating if they stop paying their mortgage.
- Consumers may stop doing business with the company at any time, accept or reject any offer the company obtains from the lender or servicer, and if they reject the offer, they don't have to pay the company's fee.

Companies are also prohibited from making any false or misleading claims about their services or those of any alternative relief providers, the likelihood of consumers getting the results they seek, or the amount of money consumers will save by using their services.

Under the federal Making Home Affordable (MHA) Program borrowers can apply for a mortgage modification if they are having difficulty paying their mortgage because their payment has increased significantly, their income has declined, or they have suffered a hardship, e.g., unexpected medical bills. There is no requirement for default. The following other requirements apply:

- The amount owed on the first mortgage must be equal to or less than $729,750.
- The mortgage must be older that Jan. 1, 2009.
- The current monthly payment is more than 31 percent of your gross monthly income
- You must be able to pay up to 31 percent of your gross monthly income on a reasonable mortgage

Two MHA options have been extended to the end of 2018. They are the Home Affordable Modification Program (HAMP) and the Home Affordable Refinance Program (HARP). HAMP is designed to bring a borrower's payments down to a more affordable level by temporarily cutting the interest rate or extending the term of the loan but without a principal reduction. HARP enables a homeowner who is current on payments but underwater to refinance the loan and benefit from lower mortgage interest rates. You can get help in understanding your options, preparing your application, and working with your mortgage company by calling a HUD-approved housing counselor at **(888) 995-4673**.

Cash-Back Scams

This scam involves credit or debit card transactions with dishonest cashiers at retailers. In it the cashier would also ring up a "cash-back" charge and pocket the cash amount. To prevent this scam make sure the transaction total on your receipt and the register matches the amount or your purchases if you did not request any cash back. And report any differences to the store manager.

Charity Scams

Scammers often pose as charities and solicit donations for emotional causes such as children with life-threatening disease, wounded veterans, police and firefighters, etc. In many instances they use a name similar to a legitimate charity to mislead donors, e.g., "American Cancer Research Society" instead of the American Cancer Society. They are also more aggressive than legitimate charities, often calling you at home or coming to your door. Keep in mind that legitimate charities, in contrast to scams, will not pressure you to donate on the spot. Any suspicious e-mails solicitations and fake websites should be reported to the FBI's IC3 at **www.ic3.gov**.

You should always beware of charities that spring up overnight in connection with current events, especially if they are tragic, or natural disasters. They may make a compelling case for your money, but as a practical

matter, they usually don't have the ability to get donations to the affected areas or people. Look for the official charity if you want to contribute. There will always be one. Look for other qualified charities by state on the website of the National Voluntary Organizations Active in Disasters (NVOAD) at **www.nvoad.org/states**. Also, never open attached e-mail files that purport to show pictures of a disaster area. They may contain viruses. Scammers capitalize on natural disasters in many ways.

With the expansion of social media, charities are now using Facebook posts and Twitter feeds to find donors. And donors are taking to social media to find and share information about charities they deem worthy. But all this sharing, if not done wisely, can leave donors vulnerable to scams. It's easy for a bogus Facebook page, blog, or Twitter feed to look authentic. This is the bad side of social media. The following tips will help protect you from a wide variety of charity scams.

- Check out any charities on the California Attorney General's website at **www.ag.ca.gov/charities.** It has a searchable database that provides information on legitimate charities.
- Also check to see if the charity is registered by going to the Attorney General's Registry of Charitable Trusts at **http://rct.doj.ca.gov/Verification/Web/Search.aspx?facility=Y**.
- You can also go to **www.CharityNavigator.org**, a popular charity-rating website that rates nonprofits on a zero- to four-star scale on how they perform over time. There you can also get the following information on specific charities: fund-raising efficiency rate, program/administrative spending ratios, revenue/expense statements, and salaries of top administrators. Most reputable charities will spend about 75 percent of their funds on their programs. Other sources of information are **www.GuideStar.org** and **www.give.org**. In the latter the BBB Wise Giving Alliance considers whether the charities on its national charity report list meet its 20 standards for charity accountability. These standards deal with governance, finances, fund raising, effectiveness, donor privacy, complaints, etc.
- Check that the charity is registered as a nonprofit with the IRS and is eligible to receive tax-deductible charitable contributions. You can do this at **www.irs.gov/charities-non-profits/exempt-organizations-select-check**. See the search tips on how to proceed.
- Also check the charity's latest IRS Form 990. That is the IRS' primary tool for gathering information about tax-exempt organizations. And by law non-profit organizations must make these tax forms available to the public for the last three years. They touch on everything from management policy and executive pay to conflicts of interest. And they will tell you whether the charity is financially secure. Copies are available for purchase from the IRS on DVD or paper. See **www.irs.gov/charities-non-profits/copies-of-scanned-eo-returns-available** for information on ordering copies or viewing them online. Copies are also available in a machine-readable format through Amazon Web Services (AWS) at **https://aws.amazon.com/public-data-sets/irs-990**. These forms can also be seen on **www.GuideStar.org** or obtained directly from the charity.
- Never donate to a solicitor who calls on the phone. Even if the charity is legitimate, most of the money will go to the telemarketing company that is being paid to make the calls. If you want to contribute, do so directly to the charity, not to the solicitor. And never give a solicitor your SSN, credit or debit card number, or any other personal or financial information.
- Never respond to online solicitations from unknown individuals. Be suspicious of individuals who represent themselves as member or officials of charitable organizations who ask for donations by e-mail or social networking sites.
- Don't respond to unsolicited e-mails, texts, or tweets. Many are fraudulent and contain malware. If you are thinking about giving online, look for indicators that the site is secure, i.e., the communications are encrypted. These are lock icons on the browser's status bar or a URL that begins with "**https**."
- Never click on links in unsolicited e-mails. They may contain viruses. If the link is to a charity, find and use its URL rather than click on a link.
- Beware of charities that don't have a website. Most legitimate charities have websites that end in **.org** rather than **.com**.
- Ask for written information about the charity's mission, how your donation will be used, and proof that your donation is tax deductible. A legitimate charity will send this to you.
- Don't be pressures into making a contribution. Legitimate charities don't use those tactics.

- Donate by check or credit card, never with cash or a money transfer. Write checks payable to the organization, not to a solicitor. Provide you credit card number only after you have reviewed information about the charity and verified its credibility. And ask the organization not to store your credit card information. Don't provide your SSN or any other personal or financial information. A charity doesn't need them.
- Never donate via links on e-mails, Facebook pages, or tweets.
- Keep a record of your pledges and contributions. Callers may try to trick you by thanking you for a pledge you didn't make. If you don't have a record of a pledge or contribution, resist the pressure to give.
- Remember that "free" goods offered as an incentive in raising funds are paid for out of your contribution, which means less money is available to the charity.
- Never donate to charities with copy-cat names, i.e., ones that are similar to but not exactly the same as one of known, reputable charities.

You may need to dig deeper in vetting small local charities. These can be very efficient in dealing with local problems. Here are some guidelines to follow.

- Examine the charity's mission statement. It should clearly state what the charity is trying to accomplish and how it works to achieve its goals. It is typically found on the charity's website. Ask for a copy if one isn't there. And being local, you can talk to the staff and find out how its funds are being used.
- Find out who's in charge. A small charity should have at least three board members to start. This will ensure that different ideas are being considered. Eventually it should have at least six board members to provide expertise in legal, financial, and other matters.
- Check its finances. Ask to see copies of its IRS Form 990, Letter of Determination from the IRS showing its tax-exempt status, audited financial statements, and annual reports.
- Ask about its conflict-of-interest policy regarding staff compensation and outside financial interests.
- Beware of any charity that is unwilling to answer your questions.

If you live in San Diego and find that a solicitor of charitable contributions has made false statements concerning the purpose or organization for which the money or property is solicited or received, or concerning the cost and expense of solicitation or the manner in which the money or property or any part thereof is to be used, you should report this to the SDPD on one of its non-emergency numbers, **(619) 531-2000** or **(858) 484-3154**. Otherwise report it to your local law enforcement agency. Such solicitations are misdemeanors under California Penal Code (PC) Sec. 532d(a).

Checks from Unknown Parties

In one case a consumer found a $9 check with a product he had ordered. He cashed the check and later found a $149 charge on his credit card. He failed to read the small print on the back of the check which authorized the transfer of his personal information to another company that would enroll him as a member of an organization for a monthly fee. To avoid such scams never cash checks from unknown parties.

Check Washing

People who steal mail are usually looking for envelopes containing personal checks that are made out to pay bills. They wash the check with chemicals to remove the payee's name and amount. The result is a blank check signed by you. They can then fill in their names and an amount and cash it. You can prevent your checks from being stolen by depositing your mail in boxes or slots inside a post office. Or use an outside box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Never leave mail for pickups from personal curbside boxes or cluster box units. And when making out checks use a pen with ink that is resistant to washing.

Chimney Sweeps

If you want your chimney cleaned and inspected to keep it operating safely and efficiently, and to keep you from getting carbon monoxide poisoning, consider using a sweep certified by the Chimney Safety Institute of American (CSIA). These sweeps have passed an intensive exam based on fire codes, clearances, and standards for construction and maintenance of chimneys and venting systems. The CSIA also recommends asking the following questions about the sweep's company:

- How long has it been in business?
- Does it offer current references?
- Does it carry a valid business liability insurance policy to protect your home and furnishings against accidents?

Also ask neighbors, friends, and family for referrals and check the company's status with the BBB. Note that a sweep that only performs cleaning does not need to be licensed. But anyone doing repairs needs a State contractor's license, the type depending on the nature of the repairs.

Counterfeit Checks

Someone sends or gives you a check and asks you to deposit it in your bank and then wire back a portion of the amount, leaving you with a net profit. This can happen in many ways and will sound like a good deal. But the check will be counterfeit. It will be returned to your bank and the full amount deducted from your account. You can avoid this problem by not cashing the check in the first place, but if you do you should wait until it clears before withdrawing any of it.

In one example of this scam letters are sent to people asking them to participate in a mystery shopping program to help evaluate a certain business in their area. A counterfeit check that appears to come from a government agency is enclosed along with instructions to deposit it in your bank, spend some at the business and provide a written appraisal of your shopping experience, keep a portion for your work, and wire the balance elsewhere, typically overseas. There are legitimate companies that hire mystery shopping but they usually pay $8 to $20 per shop after the assignment is completed, and don't require any wire transfers.

In another example a collection lawyer receives what appears to be a legitimate solicitation e-mail from a prospective client seeking representation in a debt collection matter. The lawyer then receives what appears to be a valid cashier's check, supposedly a settlement check from a debtor, from a reputable bank. After the check is cashed and the money deposited in the lawyer's client trust account, the "client" asks that the funds, less the fees, be wired to a foreign bank. The cashier's check was counterfeit and the lawyer was left holding the bag. An article in the March 2016 issue of the *California Bar eJournal* warned that scammers continue to target attorneys with check fraud. California attorneys who believe a solicitation may be legitimate and worth pursuing should follow the steps suggested in the January 2011 Ethics Alert published by the California Bar's Committee on Professional Responsibility and Conduct entitled *Internet Scams Targeting Attorneys* to protect themselves and their practices from falling victim to this scam.

In January 2007 The Office of the Comptroller of the Currency (OCC) sent out bulletin OCC 2007-2 to all national banks warning them of an increasing number of complaints relating to counterfeit cashier's checks and advising both depositary and paying banks of actions to take to address risks to them. These counterfeit checks have often been received by bank customers who sell goods or services over the Internet. And in some cases they are asked to wire other funds to third parties. In all these case the customer believes the cashier's check to be valid and deposits it in his or her account. When the bank makes the funds "available" the customer sends the goods or funds. Later the check is returned unpaid because it is discovered to be counterfeit. To avoid losses from this scam, bank customers should wait until the check clears before sending goods or funds.

The FBI's IC3 recommends taking the following steps to determine whether a check is counterfeit:

- Ensure that the amount of the check matches in figures and words.
- Inspect the check to see that the account number is not shiny in appearance, the drawer's signature looks natural, i.e., not traced, and the check is perforated on at least one side.
- Inspect the check for additions, deletions, or other alterations.
- Contact the financial institution on which the check is drawn to ensure its legitimacy. Obtain the phone number from an independent, reliable source, not from the check itself.
- Be cautious in dealing with foreigners.

More on fake checks is on the FTC website at **www.consumer.ftc.gov/articles/0159-fake-checks**. It advises the following to avoid a counterfeit check scam.

- Throw away any offer that asks you to pay for a prize or a gift. If it's free or a gift, you shouldn't have to pay anything for it.
- Resist the urge to enter foreign lotteries. It's illegal to play a foreign lottery through the mail or the telephone, and most foreign lottery solicitations are phony.
- Know who you're dealing with and never wire money to strangers.
- If you're selling something, don't accept a check for more than the selling price, no matter how tempting the offer or how convincing the story. Ask the buyer to write the check for the correct amount. If the buyer refuses to send the correct amount, return the check. Don't send the merchandise.
- As a seller you can say you won't accept payment by check. Suggest using an escrow or online payment service. If the buyer insists on using a particular escrow or online payment service you've never heard of, check it out. Don't use it if it doesn't appear to be legitimate.
- If you accept payment by check, ask for a check drawn on a local bank or a bank with a local branch. That way you can take the check to the bank to make sure it is valid. If that's not possible, call the bank where the check was purchased, and ask if it is valid. Get the bank's phone number from directory assistance or an Internet site that you know and trust, not from the person who gave you the check.
- If the buyer insists that you wire back funds, end the transaction immediately. Legitimate buyers don't pressure you to send money by wire transfer services. In addition, you have little recourse if there's a problem with a wire transaction.
- Resist any pressure to "act now." If the buyer's offer is good now, it should be good after the check clears.

Credit Card Fraud

Credit or debit card fraud occurs when someone uses one of your cards without your permission. It can happen after someone steals your card or identity. In the latter a person obtains data associated with the card account, including the card account number or other information that would be used in a legitimate transaction. A thief might go through your trash to find discarded billing statements. A dishonest clerk or waiter might take a photo of your card. Or a business might get hacked and your card number stolen and sold. Fraud occurs when the thief tries to buy things or to take money out of an account.

You can take the following are measures to prevent credit card theft.

- Don't leave your cards out in your home or office. Keep them in a secure place, especially if you have people working in your home.
- Keep your eye on your card during transactions. Make sure you get it back before you walk away.
- Never put your purse or wallet on a counter while shopping.
- Cut up old cards, cutting through the account number, before you dispose of them.
- When out:
    - Avoid carrying a purse if possible. Wear a money pouch instead.
    - Carry a purse with a shoulder strap if you must. Keep the strap over your shoulder, the flap next to your body, and your hand on the strap. Hang the purse diagonally across your body.

- When wearing a coat and carrying a purse, conceal the strap and purse under the coat.
- Keep a tight grip on your purse. Don't let it hang loose or leave it on a counter in a store.
- Carry your wallet, keys, and other valuables in an inside or front pants pocket, a fanny pack, or other safe place. Don't carry a wallet in a back pocket.
- Carry your cards separately from your wallet. This can minimize your losses if someone steals your wallet or purse. And carry only the card you need for that outing.

Measures you can take to prevent identity theft in using credit and debit cards can be found in the paper entitled *Identity Theft Prevention and Victim Responses* at **www.sandiego.gov/sites/default/files/identitytheftpreventionandvictimresources.pdf**. One measure suggested there is that you call your credit card companies when you travel to alert them about when, where, and how long you will be away. This will enable their fraud departments to stop charges if your card is used elsewhere, and reduces the risk that charges made where you are going to be will not be accepted. Or you can do this online if your card issuer has a "travel notification" or similar tab that you can use when you log onto your account. Another alternative became available in April 2015. Visa's Mobile Location Confirmation is designed to provide issuing financial institutions with more information to help protect against fraud while facilitating a better payment experience for consumers. It is described in a Visa press release dated Feb. 12, 2015 which can be seen at **http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=2016148.**

In 2012, after widespread identity theft due to weak security in the point-of-sale terminals at Target, Home Depot, and other major retailers, Visa, MasterCard, Discover, and American Express announced plans to issue new cards with Europay, MasterCard and Visa (EMV) technology. These cards have a secure microchip that is designed to make them very difficult and expensive to counterfeit. Also, the chip stores encrypted data about the cardholder account, as well as a cryptogram that allows banks to tell whether a card or transaction has been modified in any way. So when you get a new card, make sure it has the EMV chip.

Credit Repair

The 1996 Credit Repair Organizations Act prohibits a variety of false and misleading statements, as well as fraud by Credit Repair Organizations (CROs). CROs may not receive payment before any promised service is "fully performed." Services must be under written contract, which must include a detailed description of the services and contract performance time. CROs must provide the consumer with a separate written disclosure statement describing the consumer's rights before entering into the contract. And consumers can sue to recover the greater of the amount paid or actual damages, punitive damages, costs, and attorney's fees for violations of the Act.

If you encounter a CRO that promises to remove negative items from your credit reports it is safe to assume it's a scam. In exchange for a fee it will promise to pester the credit reporting companies until they wipe out your debts and bankruptcy records. It will string you along saying the process will take several months. By then you may be out hundreds or even thousands of dollars. In the meantime, debts can stay on your credit record for up to seven years, and a Chapter 7 bankruptcy can remain for up to 10 years. If you think you were duped by a CRO you should call the FTC Consumer Response Center at **(877) 382-4357**. And if you have second thoughts about signing a contract for credit repair services, you can cancel it within five days.

To keep from being scammed you should avoid any company that does any of the following:

- Wants you to pay for credit repair before they provide any services,
- Will not tell you your legal rights,
- Will not tell you what you can do on your own at no cost,
- Tells you not to contact a credit reporting company directly,
- Advises you to dispute all negative items in your credit report, or
- Suggests you create a new credit identity, e.g., by applying for an Employer Identification Number to use instead of your SSN.

Here are some things you can do to improve your credit.

- Check your credit reports regularly for mistakes or collections you didn't know about. Free copies are available annually from Equifax, Experian, and TransUnion, the three nationwide consumer credit reporting bureaus, by visiting **www.AnnualCreditReport.com**, the only site officially directed by Federal law to provide them. Contact the reporting bureaus in writing about any mistakes or disputed collections. If a mistake is confirmed you can ask the reporting bureau to send a corrected report to prospective lenders.
- Check that past-due accounts older than seven years from the first date of delinquency have been removed. Challenge any that are still on the report. Include copies of documents that support your position and a copy of the credit report. Send them to the reporting company by certified mail.
- Pay down or pay off outstanding debt. Deal with those with the highest interest rates first.
- Develop a plan to pay off high-interest credit card debts. Advice on planning is available from the National Endowment for Financial Education's website at **www.smartaboutmoney.org**. Paying the monthly minimum due is very expensive. It will also take a very long time to pay off the balance. Consider the following alternatives: (1) use savings or investments, especially those that are earning less than the debt interest rate, to pay down the balance, (2) reduce expenses in order to make greater payments, (3) take out a loan at a lower-interest rate to pay off the balance, and (4) stop charging things on the card.
- Try to negotiate a lower interest rate or late fees if you are having trouble paying a debt. Speak to a supervisor who has authority to change the terms of your loan.
- Consider seeing a credit counselor if you can't handle your debts on your own. Consultations are usually free. Two organizations that can refer you to a counselor are the National Foundation for Credit Counseling and the Association of Independent Consumer Credit Counseling Agencies. You can call the former at **(800) 388-2227** or visit its website at **www.nfcc.org**. You can call the latter at **(866) 703-8787** or visit its website at **www.aiccca.org**.
- Get a secured credit card if you need to re-establish your credit. Such a card requires a security deposit to secure your charges to it. And they usually have fees that regular cards don't have. Look for cards with reasonable fees.
- Prepaid debit cards will not help you establish a good credit history because their use is not reported to the three major credit reporting bureaus. Also, be aware that such cards come at a steep price, and while their funds are insured by the Federal Deposit Insurance Corporation (FDIC), the cards aren't protected by federal laws that limit credit card losses to $50 for fraudulent charges. Before buying a prepaid card make sure you know about all the fees and understand the small print in the cardholder agreement. There can be fees for first-time issuance, reloading, ATM usage, balance inquiries, maintenance, and replacement. This information is usually only available on the company's website. For more information on prepaid cards, see the Consumers Union paper entitled *Prepaid Cards: Second Tier Bank Account Substitutes* dated September 2010 at **www.sdut.us/prepaidplastic**.

These and other things you can do to repair your credit are explained on a page entitled *Building a Better Credit Report* on the FTC's website at **www.ftc.gov/bcp/edu/pubs/consumer/credit/cre03.shtm#scams**.

Debt Collection

Here callers say they are from a debt collection agency, law firm, bank, or government agency, and say that you owe money on a debt or a loan and need to pay immediately. Somehow they may have obtained some of your personal information like your SSN, address, employer, etc. to make the call sound legitimate. Some people who don't owe a debt will pay hoping that the harassment will stop. That's a mistake because it won't. A better response is to verify that the debt collector is legitimate. Ask the caller for his or her name, company, street address, phone number, and state license number. Say that you will not discuss any debt until you receive a written notice of it. And don't give any personal or financial information to the caller until you have verified that he or she is legitimate. Here are a few signs that signal a debt collection scam.

- The caller uses abusive, unfair, or deceptive practices to collect from you. These are prohibited in the federal Fair Debt Collection Practices Act (FDCPA). Some questions and answers about your rights under the Act can be found in an article entitled *Debt Collection* on the FTC website at **www.consumer.ftc.gov/articles/0149-debt-collection**.
- The caller refuses to give you information about your alleged debt. You have a right to ask a debt collector for a written validation of the alleged debt. If the call is legitimate, the debt collector must provide the following information to you, either in its first contact with you regarding an unpaid bill or in writing within five days after that first contact: the amount you owe, the name of the creditor, and a statement of how to dispute the bill in writing within 30 days. A guide to this and other rights you have under the California FDCPA in CC Secs. 1788-1788.33 can be found at **https://oag.ca.gov/consumers/general/collection_agencies10**. They deal with the following: harassment and call restrictions, collector contacting your employer or other people, payment arrangements, postdated checks, credit reporting, interest and other charges, and filing a consumer complaint.
- The caller refuses to give you an organization name, mailing address, phone number, and state license number. Many states other than California have licensing requirements for debt collectors. They can be found at **www.insidearm.com/state-licensing**. If a license is required, verify it with the officials in the state where it was issued.
- The caller asks you for personal financial or other sensitive information like your SSN.

If the debt collector contacts you in writing with all the legally-required information, you will be told that the debt will be assumed to be valid if you don't dispute it within 30 days. And that if you do dispute it in writing within 30 days, the debt collector will provide verification of the debt. There are different ways to respond appropriately to debt collectors, depending on your situation. If you're experiencing a common problem, you can use one of the following sample letters from the website of the Consumer Financial Protection Bureau (CFPB) at **www.consumerfinance.gov/askcfpb/ 1695/What-should-I-do-when-a-debt-collector-contacts-me.html**.

- I do not owe this debt.
- I need more information about this debt.
- I want you to stop contacting me.
- I want you to only contact me through my lawyer.
- I want to specify how you can contact me.

This website also has links to the following debt collection subjects.

- Understanding debt collection
- Harassment by a debt collector
- Getting information from a debt collector
- Disputing a debt in collection

And if you can't get your issue resolved, there's a link for you to submit a debt collection complaint. The CFPB will forward it to the debt collection company, give you a tracking number, and keep you updated on the status of your complaint.

Debt Settlement

Debt settlement, a process in which a consumer who is behind in debt payments negotiates with the creditor to pay off the debt in full for less than the amount owed, has become a big business as American consumers struggle with historic levels of unsecured debt. Problems arise when a consumer pays a debt-settlement company to do the negotiations and make the payments. In a 2010 investigation the U.S. Government

Accountability Office (GAO) found that some debt-settlement companies engaged in unscrupulous activities. These include the following.

- Charging fees before settling any debts
- Applying monthly payments to fees before reserving them for debt settlement
- Advertising that their services were linked to government programs
- Offering $100 if they could not get a consumer out of debt in 24 hours
- Claiming high success rates, up to 100 percent
- Suggesting that consumers stop paying on their debts.

Its report on this, GAO-10-593T entitled *Debt Settlement: Fraudulent, Abusive, and Deceptive Practices Pose Risk to Consumers* dated April 22, 2010, can be found online **www.gao.gov/assets/130/124498.pdf**.

If you do stop making payments to your creditors, you will damage your credit and could become the target of lawsuits. You will also be subjected to late fees and penalties, all of which might add up to more wipe out any savings from the debt settlement. And remember that any debt that is forgiven will be taxed as income.

You can avoid being scammed when seeking help with debt settlement by doing your homework and shopping around. Consider several companies. Check them out with the BBB. Go online and see what people are saying about them. Find out how long they have been in business and whether any legal actions are pending against them. And ask about their services and fees. You should also consider debt consolidation, credit counseling, and doing it yourself. The first is a process in which a consumer takes out a load to combine debts into one payment, typically smaller and at a lower interest rate than the individual debts. In the second a consumer receives credit counseling and assistance in managing finances, budgeting, and debt consolidation without a loan. The third involves the following:

- List your goals.
- List your expenses and see which ones you can reduce or eliminate.
- Call your creditors to request a lower interest rate. Do this before your debts are assigned to a collection agency.
- Put as much money as possible to reducing your debt, and keep doing it until all your debts are paid off.
- Sell any stuff you don't use to make extra money.

If you have a student loan, there are countless ads online from companies offering to help you manage your debt for an upfront fee. Some even charge a monthly maintenance fee. These fees violate federal law when they trick borrowers into paying for federal benefits. Before you sign a contract with a debt relief company you should try to get relief by yourself.

If you're a federal student loan borrower, the U.S. Department of Education provides free assistance in doing the following:

- Lowering your monthly payments. The federal government makes it easy for you to switch to a more affordable repayment plan at any time at no cost.
- Consolidating your loans. If you have multiple loans that you want to combine, you can apply for loan consolidation through **www.StudentLoans.gov**. The application is free and there are no extra processing fees.
- Seeing If you qualify for loan forgiveness. In this program a borrower is released from its obligation to repay all or a portion of the principal and interest on a student loan. It was created to encourage people to take certain types of jobs, to help borrowers with lower income jobs, and to compensate for permanent disabilities.
- Getting out of default. Even if your loan is in default, loan consolidation is free and so is getting into a loan rehabilitation plan, as discussed in **https://studentaid.ed.gov/sa/repay-loans/default/get-out**.

More information on these options is available from the official blog of the U. S. Department of Education at **http://blog.ed.gov/2015/04/beware-you-dont-have-to-pay-for-help-with-your-student-loans/**. If you're a private student load borrower, you have the same options but they must be negotiated directly with your lender. There is no federal program for this because loans vary so much from lender to lender.

Dishonest Tax Return Preparers and Related Tax Scams

Scam artists routinely pose as tax return preparers during tax time, luring victims in by promising large federal tax refunds or refunds that people never dreamed they were due in the first place. Here are some things unscrupulous or abusive tax return preparers might do.

- Use flyers, advertisements, phony store fronts, and even word of mouth to suggest that the taxpayer can get free money from the IRS by filing a tax return with little or no documentation.
- Spread the word through community groups or churches where trust is high.
- Advertise on the Internet and direct individuals to call toll-free numbers where they are asked for their SSNs.
- Offer to prepare a return and split the refund or charge a fee based on the amount of the refund.
- Promise refunds to people, including non-English speakers, who have little or no income and normally don't have a tax filing requirement.
- Build false hopes and charge people good money for bad advice.
- Make up supplemental incomes and losses, file fake Forms 1099-MISC, declare unpaid expenses as actual deductions, claim fictitious or ineligible dependents, add fictitious items in the itemized deductions, use inadmissible credits and exaggerated exemptions, and falsify supporting documents.
- Encourage taxpayers to overstate deductions and make fictitious claims for refunds or rebates based on false statements of entitlement to tax credits, e.g., for fuel taxes. These are allowed only for taxes paid on fuel to power farm equipment and some other vehicles and equipment used off-road. Consequently, this credit is not available to most taxpayers.
- File a false return in a person's name and keep the refund.
- Victimize people due a refund by promising inflated refunds based on false claims for education credits, the Earned Income Tax Credit, American Opportunity Tax Credit, and others even if the victim was not enrolled in or paying for college.

The IRS reminds all taxpayers that they are legally responsible for what's on their return even if it was prepared by someone else. Taxpayers who buy into such false returns can end up being penalized for filing false claims or receiving fraudulent refunds. Significant penalties may apply for taxpayers who file incorrect returns. These include the following:

- 20 percent of the disallowed amount for filing an erroneous claim for a refund or credit
- $5,000 if the IRS determines a taxpayer has filed a "frivolous tax return," which is one that does not include enough information to figure the correct tax or that contains information clearly showing that the tax reported is substantially incorrect
- In addition to the full amount of tax owed, a taxpayer could be assessed a penalty of 75 percent of the amount owed if the underpayment on the return resulted from tax fraud.

Taxpayers may also be subject to criminal prosecution and be brought to trial for the following actions that could lead to additional penalties and even prison time.

- Tax evasion
- Willful failure to file a return, supply information, or pay any tax due
- Fraud and false statements
- Preparing and filing a fraudulent return

You can avoid this scam as well as identity theft by wisely choosing a tax return preparer. Here is how to do this.

- Check the person's qualifications. All paid tax return preparers must have a Preparer Tax Identification Number (PTIN) from the IRS. California law requires anyone who prepares tax returns for a fee within the State of California and is not an exempt preparer to register as a tax preparer with the California Tax Education Council (CTEC) after completing 60 hours of qualifying tax education from a CTEC-approved provider, obtaining a PTIN from the IRS, and purchasing a $5,000 tax-preparer bond. (Exempt preparers are California Certified Public Accountants (CPAs), IRS enrolled agents, and attorneys who are members of the State Bar of California.) Registered tax preparers must renew their registration annually after completing 20 hours of continuing tax education. They must also maintain a valid PTIN and a tax preparer bond. The California Franchise Tax Board (FTB) has the authority to identify and penalize unregistered tax preparers. You can verify the registration status of a tax preparer at **www.ctec.org/Payer/FindVerifyPreparer/**. If you deal with an exempt preparer, ask if the person is affiliated with a professional organization like the National Association of Enrolled Agents and attends continuing education classes.
- Non-exempt tax return preparers can also participate in the IRS's new voluntary Annual Filing Season Program (AFSP), which aims to recognize the efforts of non-exempt preparers who aspire to a higher level of professionalism. To receive an AFSP Record of Completion from the IRS, tax preparers must have 18 hours of continuing education, including a six-hour federal tax law refresher course with test. AFSP participants are also included in the directory of federal tax return preparers on the IRS website. This directory will also contain the names and address of all exempt tax return preparers. More information on the AFSP is on the IRS website at **www.irs.gov/Tax-Professionals/Annual-Filing-Season-Program**.
- You can use the IRS Directory of Federal Tax Return Preparers with Credentials and Select Qualifications to search for tax preparers in your area who hold professional credentials recognized by the IRS or who hold an AFSP Record of Completion. It's online at **http://irs.treasury.gov/rpo/rpo.jsf**. Also online are tips for choosing a tax preparer at **www.irs.gov/uac/Choose-Your-Tax-Preparer-Wisely** and help learning more about the different types of tax professionals in Understanding Tax Return Preparer Credentials and Qualifications at **www.irs.gov/Tax-Professionals/Understanding-Tax-Return-Preparer-Credentials-and-Qualifications**. The latter is especially important because tax return preparers have differing levels of skills, education and expertise and anyone with a PTIN can prepare a tax return for a client.
- Check the preparer's history. See if he or she has a questionable history with the BBB, been subject to disciplinary actions by state agencies or professional organizations, and has a current license.
- Avoid preparers who guarantee a refund, base their fee on a percentage of your refund, claim they can obtain larger refunds than other preparers, or say you can walk out of their office with a check in your hand. The latter is actually a Refund Anticipation Loan (RAL) which may be usurious.
- Provide records and receipts. Good preparers will ask to see them. They'll ask questions to determine your total income, deductions, tax credits and other items. Do not rely on a preparer who is willing to e-file your return using your last pay stub instead of your Form W-2. This is against IRS e-file rules.
- Ask to have your return e-filed.
- Have any refund sent directly to you or deposited in your bank account. Never allow it to go to the preparer.
- Make sure the preparer is accessible after your return has been filed in case the IRS questions anything on it.
- Don't use a preparer who does not ask to see all the records and receipts needed to prepare your return.
- Never sign a blank return.
- Review the entire return before signing it. Ask questions and make sure you understand it. Don't use a preparer who won't sign your finished return and includes his or her PTIN. Although the preparer signs it, you are responsible for the accuracy of every item on your return.
- Get a copy of your return.

Finally, you should report tax return preparer misconduct, improper activities, and suspected tax fraud to the IRS. Use Form 14157, Complaint: Tax Return Preparer. It's online at **www.irs.gov/pub/irs-pdf/f14157.pdf**. If you suspect a tax return preparer filed or changed your return without your consent, you should also file Form 14157-A, Return Preparer Fraud or Misconduct Affidavit. It's online at **www.irs.gov/pub/irs-pdf/f14157a.pdf**.

On February 17, 2017 the IRS published a recap of its "Dirty Dozen" tax scams for 2017. Here's a summary of them with their URLs.

- Phishing at **www.irs.gov/uac/newsroom/phishing-schemes-lead-the-irs-dirty-dozen-list-of-tax-scams-for-2017-remain-tax-time-threat**. Taxpayers need to be on guard against fake e-mails or websites looking to steal personal information. The IRS will never initiate contact with taxpayers via e-mail about a bill or refund. Don't click on one claiming to be from the IRS. Be wary of e-mails and websites that may be nothing more than scams to steal personal information.
- Phone scams at **www.irs.gov/uac/newsroom/phone-scams-remain-serious-threat-no-2-on-the-irs-dirty-dozen-list-of-tax-scams-for-2017**. Phone calls from criminals impersonating IRS agents remain an ongoing threat to taxpayers. The IRS has seen a surge of these phone scams in recent years as con artists threaten taxpayers with police arrest, deportation and license revocation, among other things.
- Identity theft at **www.irs.gov/uac/newsroom/identity-theft-remains-on-dirty-dozen-list-of-tax-scams-irs-states-tax-industry-urge-people-to-be-vigilant-against-criminals**. Taxpayers need to watch out for identity theft especially around tax time. The IRS continues to aggressively pursue the criminals that file fraudulent returns using someone else's Social Security number. Though the agency is making progress on this front, taxpayers still need to be extremely cautious and do everything they can to avoid being victimized.
- Return preparer fraud at **www.irs.gov/uac/newsroom/irs-dirty-dozen-series-of-tax-scams-for-2017-includes-return-preparer-fraud-choose-reputable-return-preparers**. Be on the lookout for unscrupulous return preparers. The vast majority of tax professionals provide honest high-quality service. There are some dishonest preparers who set up shop each filing season to perpetrate refund fraud, identity theft and other scams that hurt taxpayers.
- Fake charities at **www.irs.gov/uac/newsroom/fake-charities-on-the-irs-dirty-dozen-list-of-tax-scams-for-2017**. Be on guard against groups masquerading as charitable organizations to attract donations from unsuspecting contributors. Be wary of charities with names similar to familiar or nationally known organizations. Contributors should take a few extra minutes to ensure their hard-earned money goes to legitimate and currently eligible charities. See the above section on Charity Scams for links to pages on the IRS website that taxpayers can use to check out the status of charitable organizations.
- Inflated refund claims at **www.irs.gov/uac/newsroom/falsely-inflating-refund-claims-on-the-irs-dirty-dozen-list-of-tax-scams-for-2017**. Taxpayers should be on the lookout for anyone promising inflated refunds. Be wary of anyone who asks taxpayers to sign a blank return, promises a big refund before looking at their records or charges fees based on a percentage of the refund. Fraudsters use flyers, advertisements, phony storefronts and word of mouth via community groups where trust is high to find victims.
- Excessive claims for business credits at **www.irs.gov/uac/newsroom/excessive-claims-for-business-credits-makes-the-irs-dirty-dozen-list-of-tax-scams**. Avoid improperly claiming the fuel tax credit, a tax benefit generally not available to most taxpayers. The credit is usually limited to off-highway business use, including use in farming. Taxpayers should also avoid misuse of the research credit. Improper claims often involve failures to participate in or substantiate qualified research activities and/or satisfy the requirements related to qualified research expenses.
- Falsely padding deductions on returns at **www.irs.gov/uac/newsroom/irs-annual-dirty-dozen-list-of-tax-scams-to-avoid-includes-falsely-padding-deductions**. Taxpayers should avoid the temptation to falsely inflate deductions or expenses on their returns to pay less than what they owe or potentially receive larger refunds. Think twice before overstating deductions such as charitable contributions and business expenses or improperly claiming credits such as the Earned Income Tax Credit or Child Tax Credit.

- Falsifying income to claim credits at **www.irs.gov/uac/newsroom/irs-includes-falsifying-income-scam-in-2017-list-of-dirty-dozen**. Don't invent income to erroneously qualify for tax credits, such as the Earned Income Tax Credit. Taxpayers are sometimes talked into doing this by con artists. Taxpayers should file the most accurate return possible because they are legally responsible for what is on their return. This scam can lead to taxpayers facing large bills to pay back taxes, interest and penalties. In some cases, they may even face criminal prosecution.
- Abusive tax shelters at **www.irs.gov/uac/newsroom/irs-warns-of-abusive-tax-shelters-on-2017-dirty-dozen-list-of-tax-scams**. Don't use abusive tax structures to avoid paying taxes. The IRS is committed to stopping complex tax avoidance schemes and the people who create and sell them. The vast majority of taxpayers pay their fair share, and everyone should be on the lookout for people peddling tax shelters that sound too good to be true. When in doubt, taxpayers should seek an independent opinion regarding complex products they are offered.
- Frivolous tax arguments at **www.irs.gov/uac/newsroom/irs-dirty-dozen-tax-scams-list-for-2017-continues-with-warning-against-frivolous-tax-arguments**. Don't use frivolous tax arguments to avoid paying tax. Promoters of frivolous schemes encourage taxpayers to make unreasonable and outlandish claims even though they have been repeatedly thrown out of court. While taxpayers have the right to contest their tax liabilities in court, no one has the right to disobey the law or disregard their responsibility to pay taxes. The penalty for filing a frivolous tax return is $5,000.
- Offshore tax avoidance at **www.irs.gov/uac/newsroom/irs-committed-to-stopping-offshore-tax-cheating-remains-on-dirty-dozen-list-of-tax-scams-for-2017**. The recent string of successful enforcement actions against offshore tax cheats and the financial organizations that help them shows that it's a bad bet to hide money and income offshore. Taxpayers are best served by coming in voluntarily and getting caught up on their tax-filing responsibilities. The IRS offers the Offshore Voluntary Disclosure Program to enable people to catch up on their filing and tax obligations.

Door-to-Door Solicitors

In San Diego Municipal Code (SDMC) Sec. 33.1401(a) the term solicitor is defined to mean all persons, both principal or agent, who go from house to house, or to only one house, or upon any street, sidewalk, alley, plaza, or in any park or public place in the City of San Diego, by foot or vehicle, who sell or solicit either by sample or otherwise the sale for value of goods, wares, merchandise, services, magazines, periodicals, or other publications, or subscriptions for the same, for themselves or for firms which do or do not have an established place of business in the City of San Diego or who offer to sell or distribute for value to any person any coupon, certificate, ticket or card which is redeemable in goods, wares, merchandise or services.

To protect you from becoming a victim of unscrupulous solicitors, SDMC Sec. 33.1402 requires solicitors to be registered with the SDPD and obtain an identification card showing such registration. Regulations regarding solicitors, the details of the application process, and a permit application form can be obtained on the Police regulated Business Activities page of the SDPD website at **www.sandiego.gov/treasurer/taxesfees/pdpermits/requirements**.

Identification cards are issued after applicants are fingerprinted, pass a background check, and pay the required fees. Then solicitors must wear their card on the front of their person when soliciting. The card is white in color and has a photo, tracking number, and identifying information along with an official City background. Note that persons representing nonprofit, charitable, religious, or political organizations engaged in distributing or collecting information, or polling individuals in a household do not need to register with the SDPD.

And to protect you from being pressured by solicitors into signing a contract for something you don't need or can't afford, the California Home Solicitation Sales Act requires certain disclosures by the solicitor and provides the buyer with a right to cancel any contract for goods or services costing $25 or more by giving notice in writing within three business days of signing the contract. Before asking any questions or making any statement other than a greeting, the solicitor must do the following:

- Show identification which contains the name of the solicitor, the entity he or she represents, and the address of that entity.
- Identify the trade name of the person or company that he or she represents
- Identify the kind of goods or services being offered for sale
- Clearly reveal that the purpose of the contact is to affect a sale

The solicitor must also make certain written disclosures. If they are not made, the cancellation right continues beyond the initial three-day period until the required disclosures are made. First, the contract must be in writing in the same language used in the sales presentation. And it must contain a conspicuous, statutorily-prescribed notice of the buyer's right to cancel near the space for the buyer's signature. A Notice-of-Cancellation form must be attached. For more information see *Consumers' Rights to Cancel Home Solicitation Contracts: Legal Guide K-9* at **www.dca.ca.gov/publications/legal_guides/k_9.shtml**.

If you don't want any solicitors coming to your door you can post a sign stating NO SOLICITORS or any similar language clearly denying invitation and entry to solicitors. SDMC Sec. 33.1407 states that these letters shall be at least one-half inch in height. SDMC Sec. 33.1409 then makes it unlawful for any person to ring the doorbell of a residence, rap or knock on any door or create any sound in a manner calculated to attract attention for the purpose of securing an audience with the occupant. Also in regulating solicitor conduct, SDMC Sec. 33.1410 states that no person shall operate as a solicitor between the hours 8 p.m. and 9 a.m., except by appointment.

A person going door-to-door on your street will rarely be a solicitor who meets all these city and state requirements. He or she will most likely be casing your home for a burglary, asking for money for some fictitious charity or purpose, or trying to get you to fall for a scam involving goods or services. (The following sections deal with some contractor and sales scams.) When someone rings your doorbell or knocks on your door, you should look through the peephole to see who's there. If it's a person you don't recognize, say something like "we can't come to the door now." It's important to let the person know someone is home so he or she won't try to open the door or break in somewhere else. Then if you live in San Diego, get a good description of the person and call the SDPD at **(619) 531-2000** or **(858) 484-3154**, its non-emergency numbers, to report the person as a burglary caser. Otherwise report it to your local law enforcement agency. If the person tries to open the door or refuses to leave when asked, call **911**.

Door-to-Door Solicitations by Unscrupulous Contractors

These are characterized by the following:

- Offers to do work at a reduced price. Once payment is made little or no work is done and the project is abandoned.
- Has an "office" is his or her vehicle, driving a vehicle with out-of-state license plates, using a toll-free phone number, or having no street address for his or her business
- Pressure for an immediate decision leaving no time to get competitive bids, check licenses, or contact references.
- Verbal agreements instead of a written contract.
- Offers to perform a free inspection in which serious problems that don't exist are found.
- Demand for immediate payment in cash. Unscrupulous contractors will take the money and run.
- Illegally large down payments. By law a down payment cannot exceed the lesser of $1000 or 10 percent of the project price for labor and materials. See California Business and Professions Code (BPC) Sec. 7159.5(a)(3). (There is an exception to the down payment law for about two dozen contractors who purchase blanket performance and payment bonds to protect consumers. These contractors may solicit larger down payments than those who have a basic $12,500 bond, which is required of all licensees.)

If you live in San Diego, report any suspicious solicitations to the SDPD at **(619) 531-2000** or **(858) 484-3154** with a description of the person and his or her vehicle license plate number. Otherwise, report them to your local law enforcement agency. You can avoid these scams in hiring a contractor by doing the following:

- Deal with and hire only licensed contractors. Anyone performing home improvement work valued at $500 or more in combined labor and material costs must be licensed by the Contractors State License Board (CSLB). Get the contractor's license number and verify that it is active and in good standing online at **www.cslb.ca.gov** or by calling **(800) 321-2752**. The CSLB also provides information about the licensee's certifications, bonding, workers' compensation insurance status, and any pending or prior disciplinary actions.
- The contractor should also be licensed to work in the City of San Diego, i.e., that it has a Business Tax Certificate. You can check this in the business listings on the Master Business Listing page of the City's website at **www.sandiego.gov/treasurer/taxesfees/btax/nblactive.shtml**. A local business license is not the same as a state license for a trade, skill, or area of expertise. For a state license a contractor must pass an exam, verify at least four years of journey-level experience, carry a license bond, and pass a criminal background check.
- Any contractor who is hired to remodel a home built before 1978 must be licensed and certified for lead safety by the U.S. Environmental Protection Agency (EPA). The contractor is also required to provide you with an EPA brochure on the lead safety before starting work. That brochure is available online at **www.epa.gov/lead/pubs/renovaterightbrochure.pdf**. If you remodel your own home you should refer to that brochure for precautions to take to reduce exposure to lead and asbestos during the remodeling.
- Never hire a contractor online without first checking his or her license with the CSLB.
- Ask to see the contractor's pocket license and a photo ID to verify who you are dealing with.
- Get an estimate in writing and make sure you completely understand its terms. It should include a detailed description of the work to be done, materials to be used, total cost and payment schedule, and start and completion dates.
- Get at least three bids and references from each contractor, and check the contractor's references. If possible, go see the contractor's work.
- Confirm that the contractor has a workers' compensation policy for its employees.
- Make sure that the contractor is insured. Insurance will protect you from damage caused by the contractor's employees. And consider requiring a surety bond that will guarantee that the work will be performed as stated in the contract.
- Get the contract in writing and don't sign anything until you completely understand its terms. The contract should include a detailed description of the work to be done, materials to be used, total cost and payment schedule, start and completion dates, work progress milestones, and contact information for the contractor (phone number and business address). It should also include provisions for clean-up, debris removal, and site security.
- Ask the contractor for contact information for all subcontractors and suppliers.
- For projects in the City of San Diego, call its Development Services Department at **(619) 446-5000** to determine whether permits are required and whether you or the contractor should get them. If the latter, include a provision for getting them and any needed inspections in the contract. Following a natural disaster, permit requirements may be waived if the work is necessary to correct a dangerous situation, e.g., removing a fallen tree or fixing a gas leak.
- Check with other lenders before allowing the contractor to arrange the financing for the job.
- Take your time in making a decision.
- Make sure a contract, if signed in your home, contains a three-day right to cancel provision with an attached notice of cancellation form that explains this right. If the contract is for the repair or restoration of residential premises damaged by a disaster, i.e., any sudden or catastrophic event for a state of emergency has been declared by the President of the United States or the Governor, or for which a local emergency has been declared by the executive officer or governing body of any city, county, or city, and county, you have a seven-day right to cancel. These rights are defined in California (CC) Sec. 1689.7.
- Don't pay cash and not more than the legal limit for a down payment. Beware of contractors who won't accept a check or who wants the check made out to him or her instead of the company.

- Don't let payments get ahead of the work.
- Don't make the final payment until you are satisfied with the work.
- Keep a file of all papers relating to the project, including payments.
- Go to the Guides and Pamphlets page of the CSLB website under QUICK HITS for information about traveling contractor scams and safe contracting. For the latter you should read the pamphlet entitled *What You Should Know before Hiring a Contractor*.

Door-to-Door Solicitations by Unscrupulous Contractors after a Disaster

In rebuilding after a fire or other natural disaster beware of unscrupulous contractors going door-to-door selling debris removal and construction services. Be sure to check for licenses. California BPC Sec. 7028.16 makes it a crime to contract without a license in a declared disaster area. Debris-removal contractors must have a CSLB-issued C-21 Building Moving/Demolition Contractor license. Home builders must have a B General Building Contractor license. Also, anyone who claims to be a consultant for an insurance, demolition, or construction company must be licensed. In any case, don't rush into repairs or rebuilding. Consider all your options. A good contractor will let you check things out before you make a decision.

The following tips and those in a later section on unscrupulous contractors will help you avoid scams and other problems in rebuilding after a disaster.

- Don't give any personal information such as a SSN or driver license number, or insurance information to anyone who contacts you. Keep a log of the names of the people you speak to along with dates, times, and a summary of what you discussed.
- Contact your insurance company immediately to report any loss. Follow its instructions and don't clean up until you are told to do so. Take photos of any damage right away.
- You don't have to pay any processing fees to secure disaster relief. Anyone who says you do is a scammer. And when you've been provided disaster relief funds, do not give any money to people claiming to work for government agencies. Legitimate state and federal workers should never ask you directly for money as compensation for performing inspections or filling out forms. And if you are told that you can get your insurance settlement or disaster relief funds faster if you pay a fee, don't believe it. No one can accelerate the process. And no one needs your SSN except the government agency that is providing your disaster relief funds. You'll only need to provide it once when you first register with the agency handling the funds.
- After a state of emergency is declared it is illegal for individuals or businesses to increase prices of essential goods and services by more than 10 percent unless they can prove it was due to an increase in their supplier's price. The prohibition on price gouging after a disaster applies to consumer food and services, goods or services used for emergency cleanup, supplies, medical supplies, home heating oil, building materials, housing (residential month-to-month rentals), transportation, freight and storage services, and gasoline or other motor fuels. In addition, it is a misdemeanor during 30 days following the state of emergency proclamation for a hotel or motel to increase regular rates. Report price gouging to the District Attorney's Consumer Protection Unit at **(619) 531-4070**.
- Beware of individuals who offer to remove debris from your property and ask for payment in advance. They may disappear with your money and not do any work. Or they may remove debris and dump it on some nearby property. Then you may then be responsible for the cost of removing it and possible penalties. Be sure you know where the debris is being taken and provide payment only after the job is completed.
- All public insurance adjusters must be licensed by the California Department of Insurance. Beware of unlicensed adjusters. Also beware of an adjuster who recommends a specific contractor. The adjuster may get a kickback that is added to the cost of the work.
- Beware of free offers to test your water. A dishonest company will falsely say your water is unsafe to drink and try to sell you overpriced or useless water treatment devices. If your water is from a public water utility, it can tell you about water problems and how to deal with them. If it's from a private well,

the County Health Department can answer questions. Keep in mind that no single device can solve every water quality problem.
- Beware of people represent themselves as intermediaries who claim for a fee they can arrange low-interest loans, secure relief grants, and expedite insurance adjustments and claims.

Door-to-Door Sales of Home Security Systems

These scams involve aggressive, door-to-door salespeople who make limited-time offers and use scare tactics to pressure homeowners into buying a new or upgraded home security system. For homeowners with an existing system they promise to pay any fees for terminating a long-term contract. These fees are usually not paid and the homeowner is left with monthly bills for two contracts. You can avoid these scams by doing the following.

- Beware of any door-to-door solicitors selling home security systems. Check their SDPD photo registration cards and company identification. And call their company to verify their identity before talking to them.
- Ask to see the solicitor's California Bureau of Security and Investigative Services (CBSIS) registration card, and alarm agent's identification card and license. Then check the license online at **www.breeze.ca.gov/datamart/loginCADCA.do;jsessionid=DC4C07737547B197333732C989DD8D18.vo25** or call the California Department of Consumer Affairs at **(800) 952-5210**. (Licensees have to undergo a criminal history background check through the California DoJ and the FBI.)
- Don't believe anything a solicitor says about crime in your neighborhood. Go to **www.crimemapping.com** for crime information in the past 180 days. First click on California and then on San Diego Police. Then you select from up to 15 types of crimes, a date range, and enter an address. Then click on Search to get a map and select a search radius. You can also generate a report that lists all the mapped crimes.
- Don't be pressured into any decisions. Legitimate offers are not time-sensitive.
- Get written estimates from several companies.
- Read the entire contract, especially the fine print. Make sure all oral promises are included, especially any that deal with terminating your present contract. Also make sure you understand all the costs, which could be for an expensive long-term monitoring agreement.
- Remember that you have the right to cancel any contract you sign in your home or at a location that is not the seller's permanent place of business within three days if the amount involved is $25 or more. This is the FTC's so-called Cooling-Off Rule.

For more information read the CBSIS's *Consumer Guide to Alarm Companies* at **www.dca.ca.gov/publications/alarm_companies.shtml** and the alarm company fact sheet at **www.bsis.ca.gov/forms_pubs/alarm_fact.shtml**.

Duct Cleaning

A common contractor scam begins with a low-cost air duct inspection or cleaning. A dishonest contractor may then say your ducts are filthy and contaminated with black mold, which costs about $500 to kill with ultraviolet light. Others may also suggest that you need a complete furnace or air duct cleaning which costs about $400, and a replacement air filter that costs over $100. The U.S. EPA says that most air duct cleaning is unnecessary. Dust can collect on the air returns but they can be vacuumed easily. And filters can be replaced inexpensively. The whole job should cost less than $75. Any service costing more than a few hundred dollars is probably a scam. Men who do this often arrive in an unmarked vehicle, don't wear a company uniform, use high-pressure sales techniques to scare you, and leave without providing a receipt for work done. Duct cleaning is should be considered only if you can answer YES to the following Questions:

- Are there known or observed contaminants in the ducts? These include visible mold, vermin, and dust and debris release during a home remodel.
- Have you confirmed the type and quantity of the contaminants based on testing or observation?

- Are the contaminants or their by-products capable of entering occupied spaces?
- Have you identified and controlled the source of the contaminant?
- Will duct cleaning effectively remove, inactivate, or neutralize the contaminant?
- Have you considered other options such as removal of the affected ductwork?
- Is duct cleaning the only or most effective solution?

If you decide to have your ducts cleaned, hire a contractor licensed with a C20 classification, i.e., for Warm-Air Heating, Ventilating, and Air-Conditioning (HVAC). Get the contractor's license number and verify that it is active and in good standing online at **www.cslb.ca.gov** or by calling **(800) 321-2752**. If the duct cleaner says you have a mold problem, have this verified by a mold expert.

The EPA states that a professional duct cleaning can cost between $450 and $1000 because it requires many hours and several workers. For more information about whether your home needs a HVAC duct cleaning and on choosing a contractor, see the EPA publication *Should You Have the Air Ducts in Your Home Cleaned?* It's online at **www.epa.gov/iaq/pubs/airduct.html**.

Earned Income Tax Credit

This scam targets low-income working families and individuals who: (1) don't have to file federal income tax returns because their gross income is below the filing requirement in Table 1 of IRS Publication 501, (2) qualify for the Earned Income Tax Credit but don't know about it, and (3) haven't filed for the credit. The scammers say they will file for them give them a check for a small amount, say $400. The victims don't realize that if they had filed for credit themselves they would receive more than $400. The scammers keep the difference. They also file for credits in prior years. All the victims are asked to do is provide their SSNs and sign the bottom of the form. The scammer then puts his or her address on the form and receives the full credit due. By signing a false form the victims not only lose some credits but may be liable to pay the money back with penalties. Any offer to file for this credit is a scam and be refused. People who qualify for this credit can get free assistance from the IRS at its San Diego Office at 880 Front St. It's open Monday through Friday from 8:30 a.m. to 4:30 p.m. You can call **(619) 615-9555** for an appointment.

Ecclesiastical Crime

Churches, unfortunately, provide fertile ground for scammers and con artists. The Center for the Study of Global Christianity at the Gordon-Conwell Theological Seminary estimated that of the $569 billion to be donated to Christian causes world-wide in 2012, about $35 billion or six percent will end up in the hands of embezzlers, tax evaders, money launderers, or unscrupulous ministers. Here are some things to do to make sure your donations go to the right place.

- Ask how the donation will be used. Defensive or evasive behavior and an unwillingness to answer questions indicate that the funds might be misappropriated.
- Ask to see the church's audited financial statements. Churches, unlike other nonprofit organizations, aren't required to file IRS Sec. 501(c)(3) tax forms so potential donors cannot easily get information on the church's finances and management. You have to ask for it. Start with the church's finance committee. Ask to see its financial reports and attend a finance committee meeting.
- Ask how the church receives and disburses funds. One person should not have complete control of them. The church should have a professional accounting system to ensure that the funds are handled properly.

Once you're satisfied that your donation will go to the right place, you should make sure that you can afford to make it. You shouldn't put your family into debt in the process. Some churches make giving very easy by automatically charging pledges to your credit card. To avoid debt problems you may want to get help from a financial advisor in developing a budget and fitting donations into it. A budget can also help you deal with additional requests for money from the church during the year.

Empty Box Bargains

In this scam parking lot or street hawkers offer the hottest electronic gadgets for rock-bottom prices from the back of a truck or van. They'll show you samples of their wares but your purchase will be in a sealed box. When you get home and open it you'll find it empty except for some weights. You can protect yourself from this scam by not buying anything from someone in a parking lot or on the street, no matter how good the price sounds. If the deal sounds too good to be true, it usually is.

Energy Saving Upgrades

Door-to-door sales and mailers advertising solar products, energy efficient windows, and other energy upgrades with rebates and various financing options may sound good but many have problems that can end up costing far more than originally quoted. Some contractors misrepresent the terms of loans and use a cell phone or tablet computer to obtain an electronic signature, providing no paper documents and giving the consumer no time to review the terms. Often consumers are not aware that the financing becomes a lien against their home and can adversely affect their current mortgage, ability to refinance, and the future sale of the home. And they are surprised to find the loan payments will be added to their property tax bill for 10 to 20 years. Before entering into any energy upgrade agreement or loan ask questions and make sure you understand all of the terms. Make sure you have documents you can review and take the time to review and understand them. If you can't get the documents you need or are being pressured into signing before you are ready, walk away from the deal.

If you are considering a Property Assessed Clean Energy (PACE) loan to cover the initial costs of a solar system, you should go to the Department of Energy website and read the *Best Practice Guidelines for Residential PACE Financing Programs* dated Nov. 18, 2016 at **https://energy.gov/sites/prod/files/2016/11/f34/best-practice-guidelines-RPACE.pdf**. It deals with consumer and lender protection, compatibility of PACE with other energy efficiency programs and services, minimum contractor requirements and performance standards, quality assurance and anti-fraud measures, and evaluation of program outcomes, including cost effectiveness, energy savings, and non-energy benefits such as improved health and comfort.

Fake Festivals

Looking for a good time and good eats at a good price? Getting a good deal on a food festival or other event is terrific. But don't let scammers leave a bad taste in your mouth by taking a big bite out of your money and giving you nothing in return. While there are many legitimate festivals advertised online, there are scammers who promote fun-and-food-filled days of crab feasts, concerts, and similar events. People buy the tickets but when they show up at the so-called venue, they find nothing there but other victims of this scam.

Here ways to spot and avoid fake festivals.

- Check it out**.** Type the name of the festival and/or its promoters in your search engine along with the words "scam," "fake," or "fraud." Avoid it if you see that others have been scammed.
- Search for online reviews. Avoid the festival if there aren't any.
- Check out any contact information on the website. If there's an e-mail address or phone number, try them out. Avoid the festival if you don't get a response in a reasonable time. And be wary if there isn't any contact information. But don't click on any links on the website. You could get malware in your computer.

Fake Insurance Tax Form

On October 12, 2017 the IRS alerted tax professionals and their clients to a fake insurance tax form scam that is being used to access client's annuity and life insurance accounts and steal client's e-mail addresses. This

alert can be seen at **www.irs.gov/ newsroom/fake-insurance-tax-form-scam-aims-at-stealing-data-from-tax-pros-clients**. In this scam the cybercriminal uses a phishing e-mail to get access to the tax professional's account which contain the e-mail addresses. The cybercriminal then impersonates the tax professional and sends e-mails to their clients, attaching a fake IRS insurance form and requesting that the form be completed and returned to an e-mail address very similar to the tax professional's one. The cybercriminal, using data from the completed forms, impersonates the clients, contacts their insurance companies, and attempts to make loans or withdrawals from those accounts. You can avoid this scam by contacting your tax professional in person or by phone to confirm any request to complete and return forms. But don't use any phone numbers or links in the e-mail you received for this.

Fraudulent Locksmiths

If you are not careful in selecting a locksmith you may be overcharged for simple jobs, get charged for unnecessary expensive jobs, and have faulty work done. Fraudulent locksmiths are usually unlicensed, unprofessional, and do the following:

- Advertise online and in Yellow Pages with false addresses and **800** or other toll-free phone numbers
- Operate through an out-of-town call center with local subcontractors handling the job
- Answer the phone with a generic phrase instead of a specific company name
- Quote low prices on the phone
- Use intimidating tactics and ask for more money when they arrive
- Say they have to drill and replace the lock
- Drive unmarked vehicles
- Require payment in cash

You should do the following to avoid problems in hiring a locksmith.

- Find a reputable, local locksmith before you need one. Get references from friends and neighbors. If any are recommended, check to see that they are licensed. You can do this online with CBSIS at **www.breeze.ca.gov/datamart/loginCADCA.do;jsessionid=DC4C07737547B197333732C989DD8D18.vo25** for companies and company employees. (Licensees have to undergo a criminal history background check through the California DoJ and the FBI.) If none are recommended you can search for one on the website of the Associated Locksmiths of America (ALOA). It is an association of certified locksmiths who represent the highest level of professionalism, experience, and reliability in the industry. Go its website at **www.aloa.org**, click on Find a Locksmith, and enter a ZIP code and a search radius. After selecting a locksmith check the status of its license with the CBSIS. You can also check on the company with the BBB at **www.bbb.org/sdoc**. There you can see whether it is accredited and check its rating, reason for the rating, the number of closed complaints in five categories, and since May 2012, detailed information on consumer complaints, the responses a business made to the complaint, and subsequent correspondence between the consumer, the business, and the BBB. (The names of consumers who complain will still be kept confidential.)
- Leave a duplicate house key with a neighbor or a nearby family member. If you're locked out of your house, call them first.
- Have roadside assistance included in your auto insurance. It usually includes emergency services from pre-approved companies for unlocking cars, jump-starting batteries, changing flat tires, delivering gasoline, and towing. If you're locked out of your car, call for assistance first.
- If you call a locksmith for a car or home lock-out, get an estimate for the total cost of the work, including possible extra charges for responding at night, mileage, and any other fees. Most legitimate locksmiths will give you an estimate on the phone. If the price the locksmith asks when he arrives doesn't jibe with the estimate you got on the phone or if you're told that the lock has to be drilled and replaced, don't allow the work to be done. A legitimate locksmith has tools and education that enables him or her to unlock almost any door.

- Find out if the locksmith is insured when you call. If your property is damaged during a repair, or if faulty work leads to loss or damage, it's important for the locksmith to have insurance to cover your losses.
- When the locksmith arrives ask for identification, a business card, and a license. Some locksmiths will work out of an unmarked car for emergency jobs, but most will arrive in a service vehicle that is clearly marked with their company's name.
- Before authorizing any work check to see that the invoice includes the company's name, and whether the locksmith's vehicle has a name that matches the business card, invoice, and/or bill. And never sign a blank form authorizing work.
- Expect the locksmith to ask you for identification as well. A legitimate locksmith should confirm your identity and make sure you're the property owner before doing any work.
- After all the work is completed, get an itemized invoice that covers parts, labor, mileage, and the price of the service call.

Free Airline Tickets

In this scam you get a letter from a fictitious airline with a name that's close to that of a real airline, e.g. US Airlines, which is close to US Airways. The letter says that you have been awarded two round-trip tickets and that you have to call a given phone number to claim your tickets. When you call you are immediately asked for personal and financial information. Then you are told that the tickets are no longer available but that you can save a great deal on tickets, hotels, and other things in the future if you join a travel club, which you can learn more about if you attend a free dinner and hear a sales pitch. Like the airline, the travel club is also fictitious. And if join you'll also lose your "membership" fee. So don't respond to this scam. Remember the adage, if it's too good to be true it usually is.

"Free" Trial Offers

After using your credit card to pay $5 to cover handling and shipping costs, you receive the "free" sample product you ordered. A few weeks later you receive a larger bottle of the product along with an invoice stating that $75 has been charged to your credit card. By failing to read the cancellation policy in the terms and conditions for ordering the "free" sample, you were enrolled in the company's monthly automatic shipping program.

Other "free" trial offers enroll you in clubs or subscriptions. For example, a company might offer you an introductory package of free books, CDs, magazines, or movies. If you sign up, you may be agreeing to enroll in a club that will send you more products and bill you until you cancel, or to a subscription that's automatically renewed each year.

The FTC says you can avoid the costs that might be hiding in "free" trial offers by doing the following.

- Research the company online. See what other people are saying about the company's "free" trials. Complaints from other customers can tip you off to problems that might arise with the trial.
- Read the terms and conditions of the offer. That includes offers online, on TV, in the newspaper, or on the radio. If you can't find them or can't understand exactly what you're agreeing to, don't sign up.
- Look for who's behind the offer. Just because you're buying something online from one company doesn't mean the offer isn't from someone else.
- Watch out for pre-checked boxes. If you sign up online, look for already-checked boxes. They may indicate your consent to buy more products or extend your subscription after the "free" trial ends.
- Mark your calendar. Your "free" trial will have a time limit. You need to tell the company to cancel your trial before it passes to avoid being billed for more products.
- Find out how you can cancel shipments or services you don't want. Can you return the products to avoid being charged? Do you have a limited time to respond?
- Read your credit and debit card statements carefully. That way you'll know if you're being charged for something you didn't order. If you see charges you didn't agree to, contact the company directly to sort

out the situation. If that doesn't work, call your credit card company to dispute the charge. Ask the credit card company to reverse the charge because you didn't actually order the additional products or services.

Gift Card Draining

These scams can occur several ways. In one the scammers use an inexpensive mag-strip scanner to read and store the serial numbers of preloaded gift cards. In another, they remove the cards from their packaging and copy the numbers by hand. If there's a PIN, they steal that too. Then they replace the card and go on a shopping spree by draining the balances on the cards. If the cards are not preloaded, they can call the **800** number on the card every few days to check the balance and spend it before the customer does. Here are some ways you can protect yourself from these and other gift-card scams.

- Don't buy cards from online auction sites. Some may be real but many are stolen, counterfeit, or used. It's not worth the risk.
- Only buy cards from the store issuing the card, or from a secure retailer's website. If you buy a card online, buy it from the place that you plan to use it.
- Don't buy cards from publicly displayed racks in retail stores.
- Only buy cards that are behind a customer-service desk. But don't assume that cards that are inaccessible to the public are safe. Store employees can also participate in scams.
- Carefully examine both the front and back of a card before you buy it. If the PIN is exposed, put the card back and get a different one. If the card or its packaging looks like it could have been tampered with, don't buy that card.
- Ask the store cashier to scan a preloaded card while you watch to make sure its full value is on it. This will protect you from crooks who exchange worthless cards for the cards you think you are buying.
- Keep your receipt as a proof of purchase as long as there is money stored on the card. Many retailers can track where the card was purchased, activated, and used. If the card is stolen, some retailers will replace it for you if you have the receipt.
- Register the card at the store's website. Although not all stores offer this option, you can uncover any misuse of your card sooner if it's registered.
- Never give your SSN, date of birth, or any other unneeded private information when you purchase a card. No reputable company will ask for this info.
- Use a card as quickly as possible after activating it. Don't let it sit around unused.

Government Grants

In these scams the caller will say he or she is from a government agency, e.g., the National Institutes of Health (NIH), and that you have been selected to receive a government grant, which might be for education, home repairs, medical expenses, or some other personal use. All you need to do is pay a small, one-time processing fee by wire transfer or a prepaid debit card. Or the grant will be held for you until you provide your credit card or bank account number. The scammer may also spoof your Caller ID to make it show the agency number.

Don't be fooled. You can tell it's a scam right off because no legitimate federal government employee will ever call you and say that you've qualified for or been awarded a grant you never applied for. Furthermore, there are no fees associated with applying for or receiving a government grant and all government grants are for projects with a public purpose and are for personal use. If you get any call about a government grant you never applied for, hang up. Don't even say anything. And in general, for any phone calls you did not initiate, never give out any account information or wire money or use a prepaid debit card to pay for anything.

You can get more information on government grants and avoiding scams involving them on the U. S. Department of Health & Human Services website at **www.hhs.gov/grants/grants/avoid-grant-scams/index.html**.

Green Dot MoneyPak Cards

Green Dot MoneyPak cards themselves are legitimate products when used for the right purposes. Once purchased at a participating retailer with cash, consumers can use MoneyPak cards to reload other prepaid cards, add money to a PayPal account without using a bank account, or make same-day payments to major companies. They work just like cash and transactions with them cannot be traced or reversed. Because the cards can only be bought with cash, consumers never need to disclose their personal or financial information to a retail cashier or to make a payment. Scammers prefer that their victims pay with a MoneyPak card instead of a wire because they don't have to show up at an office to claim the funds. So beware of anyone who will only accept payment by a MoneyPak card – it's probably a scam. And never give anyone the 14-digit number found on the back of the card. They can drain the card of all its funds.

Green Energy Conservation

With billions in stimulus money being released by the Federal Government for green energy programs, millions of Americans are considering home improvements that will save energy and give them tax credits of up to $1,500. To avoid being victimized by scammers who are trying to cash in on this, homeowners should keep the following in mind.

- Not all improvements qualify for tax credits. Those that do qualify are listed on **www.energystar.gov/taxcredits**.
- Don't accept any offer to file the "necessary paperwork" for a fee. You can easily do it yourself.
- Ignore any e-mail from the U.S. Department of Energy promising a refund. And don't open its attachment, which could unleash malware in your computer.
- Don't let any people into your home to do energy audits or make energy-saving repairs. Scammers often pose as local utility company employees to do this. In taking advantage of legitimate rebate programs, call the company first to set a time for an employee come to your home.
- Don't fall for high-pressure sales pitches for energy-saving devices. They don't work.
- Beware of unscrupulous contractors. See the separate section below on ways to avoid their scams.

Health-care Credit Cards

When unexpected medical expenses come up and you don't have the money to pay for them, a medical care provider may suggest you obtain and use a special credit card to pay for them. These so-called health-care credit cards will cover part or all of the expenses but they are not without risk. To entice you, they offer "no interest" for a promotional period. At the end of this period if you haven't paid the balance off in full, all the accrued interest from the date you signed up for the credit along with the unpaid balance become due. Furthermore, these cards can have a very high interest rate. A rate of 26.99 percent was being charged by CareCredit, a subsidiary of GE Capital Retail Bank, before the CFPB, in December 2013, ordered a refund of millions to consumers who were victims of their deceptive credit card enrollment tactics. See the page on the CFPB's website entitled *CFPB Orders GE CareCredit to Refund $34.1 Million for Deceptive Health-Care Credit Card Enrollment* at **www.consumerfinance.gov/about-us/newsroom/cfpb-orders-ge-carecredit-to-refund-34-1-million-for-deceptive-health-care-credit-card-enrollment** for more information about this order.

Here are some ways to avoid this scam.

- If your medical care provider suggests getting a health-care credit card to pay for its services, don't rely on its explanation of the terms of the credit. Ask for a printed copy of the application and read it carefully.
- Be sure you understand the terms and the interest rate after the promotional period.
- If you decide to get the card, make a keep a schedule for your payments so you'll have paid the entire balance by the end of the promotional period.
- Consider options with a lower interest rate if you can't pay off the balance by the end of the promotional period.

Health Insurance Fraud

The passage of the 2010 health insurance reform bill has provided scam artists and criminals with an opportunity to confuse and defraud the public by selling phony insurance policies. Scammers are now going door to door in some areas urging consumers to obtain coverage in a non-existent "limited-enrollment" period that they falsely state was made possible by the new legislation. They are also setting up toll-free phone numbers and using the Internet to sell phony policies and threaten people that they will go to jail unless they have health insurance. Consumers need to inform themselves about the new legislation and the availability of new options. They should also check whether the insurance company and the person selling the insurance are licenses, as suggested above in preventing predatory insurance sales practices. Also, any person selling door to door in San Diego should be wearing a SDPD-issued photo-ID registration card. Solicitors without this card should be reported to the SDPD on **(619) 531-2000** or **(858) 484-3154**, its non-emergency numbers. Medicare enrollment and Medicare and Medi-Cal services fraud are covered separately in later sections.

High-Pressure Sales of Financial Products at Free-Meal Seminars

Many financial services firms sponsor sales seminars and offer a free meal to entice attendees. While these seminars are advertised as educational workshops at which "nothing will be sold," they are actually held to get attendees to open accounts and buy investment products, if not at the seminar itself, then in follow-up contacts. In a 2007 study of these seminars by the U.S. Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and state securities regulators, it was found that about half featured exaggerated or misleading advertising claims and about one-quarter involved unsuitable investment recommendations. Attendees need to understand that these seminars are primarily sales events and that all claims and recommendations should be evaluated with great care before taking any actions. See the tips on spotting and avoiding most types of investment scams in the section entitled Investment Opportunities below.

High School Diploma

There are plenty of good reasons to get your high school diploma as an adult. It can open doors to a new job or promotion, or help you get into college or the military. But before you start looking into your options, you should be aware of companies that promise fast diplomas equivalent to the well-known General Educational Development (GED) online. They say that all you need to do is take a test and pay a small fee, usually a few hundred dollars. There are no classes, no study materials, and no homework, just one simple multiple-choice test on the site. The "diploma" you would get is worthless. Here's how you can spot a high school diploma scam:

- You have to pay for a diploma. It's OK to pay for classes or testing, but not for just a diploma.
- You can get the diploma from home. You don't have to take any classes or tests.
- The company claims to be affiliated with the federal government. The federal government doesn't regulate high school equivalency diploma programs. Each state decides what equivalency tests and programs are approved.
- The company claims that a wide range of organizations accept its diploma.

HVAC Tune-Ups

In this scam you respond to an ad offering a low-cost HVAC tune-up. When the contactor arrives and looks at your unit he or she says you need to replace it as soon as possible. Warning signs of this scam are the following:

- Hard-sell tactics
- Low-price for the advertised tune-up
- No address on the contractor's ads or business cards
- Contractor not available all year

Do the following to avoid getting scammed:

- Make sure the contractor has a CSLB-issued license.
- Go to the CSLB and BBB websites to check the contractor's standing and find out if there are any pending disputes or disciplinary actions.
- Get written estimates from at least three contractors. If you considering installing a whole new system, an experienced contractor should be asking you about the number of windows in your home, how many people live there, the type of insulation you have, etc.
- Get professional references for each contractor.
- Make sure that the contract includes the notice of the three-day right to cancel, and says that the contractor will obtain all permits and that inspections must be completed by the City Development Services Department to meet California energy efficiency laws.
- Make sure the contractor has worker's compensation insurance and is bonded.
- Don't pay more than 10 percent or $1000, whichever is less, as a down payment. And don't pay in cash or let your payments get ahead of the work.

Immigration Services

Navigating U.S. immigration laws can be complex. Missing a deadline, submitting the wrong forms, or making false statements can jeopardize a person's immigration status, result in the rejection or denial of benefits, make it harder to remain in the United States legally, and in some cases, result in criminal prosecution. Unauthorized immigration services providers and scam artists look for ways to exploit immigrants, and often take their money while doing nothing for them. They sometimes charge for blank government forms, say they have a special relationship with the government, or guarantee to get you results. They may promise to get you a winning slot in the Diversity Visa lottery if you pay a fee. They might charge a lot of money, supposedly to guarantee temporary protected status or get you benefits you don't qualify for. And they might use the personal information you provide to steal your identity. They are very clever about finding ways to cheat people.

Because immigrants with limited English language proficiency often are targeted by scammers the FTC has developed education materials in Arabic, Chinese, Creole, English, Korean, Russian, Spanish, and Vietnamese. These materials explain how to avoid and report immigration scams and how to find legitimate no- or low-cost immigration advice from authorized providers. They are on the FTC website at **www.consumer.ftc.gov/features/feature-0012-scams-against-immigrants**.

Information on avoiding common immigration scams is also available on the U.S. Citizenship and Immigration Service (USCIS) website at **www.uscis.gov/avoid-scams**. These deal with *notarios públicos*, payments by phone or e-mail, winning the visa lottery, scam websites, job offers, and scams targeting students.

Here are some ways to avoid immigration scams suggested on these and related websites.

- Hang up on anyone who calls saying they are from the USCIS or any other government agency. They won't call regarding immigration matters. But scammers will, usually spoofing the real USCIS or other agency's phone number, meaning that it shows up on your caller ID even though the scammers are calling from an entirely different number. If you don't hang up they will ask for sensitive personal and financial information, demand payment, or threaten you with deportation, arrest, or other negative consequences if you don't comply. Payment is usually demanded by a wire transfer, prepaid debit card, or some other means like sending cash – once is gone you can't trace it or get it back. After you hang up you should

report the call to the real USCIS at **(800) 375-5283**. Tell them what happened. They'll tell you what to do next.
- Never reply to an e-mail regarding immigration matters. And don't click on any links in it. Just delete it.
- Don't deal with anyone who offers to help solve your immigration or employment problem for a fee, which may be many thousands of dollars. In 2017 three men who claimed to be DHS agents were accused of scamming more than 150 people this way and pocketing $6 million.
- Don't go to a *notario, notario público*, or a notary public for legal advice. Although some notaries might also be attorneys, i.e., lawyers that are members of The State Bar of California, they are not allowed to give you legal advice when acting as a notary. And as such they cannot act with the USCIS or the Board of Immigration Appeals (BIA) on your behalf. Go to a licensed attorney or a registered immigration consultant, as suggested below.
- Get immigration information and forms from the USCIS website at **www.uscis.gov/portal/site/uscis**. You can download forms there for free, though you'll probably have to pay when you submit them to USCIS. Unauthorized service providers and scammers usually design their websites to look official. Their URLs end in "**.com**." They will charge you for forms and other services you can get yourself. If you don't use the Internet you can get free immigration forms by calling USCIS at **(800) 870-3676**, or by visiting the USCIS field office in San Diego at 880 Front Street.
- Don't let anyone keep your original documents, like your birth certificate or passport. Scammers may keep them and charge you to get them back.
- Never sign a form before it has been filled out, or a form that has false information in it.
- Never sign a document that you don't understand.
- Keep a copy of every form you submit, as well as every letter from the government about your application or petition.
- Keep the receipt you'll get from USCIS when you turn in your paperwork. It proves that USCIS received your application or petition. You will need the receipt to check on the status of your application.

Choosing the right person to help you is almost as important as filling out the right form, or filling it out the right way. The only people who can help you with legal matters are lawyers who are licensed to practice in state and federal courts, and accredited representatives. They will help protect you from people who will cheat you. It is against the law for others to give legal advice.

To check that someone is a licensed lawyer, and to find out if a lawyer has been disciplined, suspended, or expelled by the State Bar:

- Visit the State Bar website at **www.calbar.ca.gov** and enter the person's name in the Attorney Search box to see the person's bar membership record.
- Visit the U.S. DoJ website at **www.justice.gov/eoir/discipline.htm** to see a list of currently disciplined practitioners.

To find a lawyer in your area who specializes in immigration matters:

- Visit the American Immigration Lawyers Association website at **www.ailalawyer.com**. There you can also get answers to many frequently asked questions, including ones about the costs and qualifications of an immigration lawyer.
- Visit the State Bar of California website at **https://members.calbar.ca.gov/search/ls_search.aspx** to conduct a search for a State Bar certified specialist. Select Immigration & Nationality Law and a County from the drop-down menus to get a list.

To find an immigration lawyer who provides free or low-cost legal services for immigrants and refugees:

- See the list of free legal service providers in California from the U.S. DoJ website at **www.justice.gov/eoir/file/ProBonoCA/download**.
- Call USCIS at **(800) 375-5283** to ask about lawyers in your area.

- See the National Legal Services Directory by state on the Immigration Advocates' website at **www.immigrationadvocates.org/nonprofit/legaldirectory/**.

Accredited representatives are people who are authorized by the U.S. government to give legal immigration advice and represent you in immigration courts. They are not lawyers but work for an organization that's officially recognized by the U.S. government. They may charge a fee to help you. Both the accredited representatives and these recognized organizations are on a list kept by the BIA in the U.S. DoJ. You can see this list by state on the DoJ website at **www.justice.gov/eoir/statspub/raroster_files/raroster_orgs_reps_state_city.htm**.

In addition to lawyers and accredited representatives, in California you can get non-legal help from immigration consultants, notaries public, paralegals, and some others. The latter include law students and *reputable individuals*. Law students must be supervised by a lawyer or an accredited representative. *Reputable individuals* are known to the USCIS and must sign a legal document saying they won't take money for helping people. Be wary of a friend, your pastor, a teacher, or a relative who try to help you. They can mean well but can cause problems for you later.

If you want to hire an immigration consultant rather than an attorney it's important to understand what they can and can't do for you. Immigration consultants are people who can help consumers fill out paperwork and translate and submit forms to government agencies. Immigration consultants in California can't give anyone legal advice and can't represent you in Immigration Courts. Attorneys or accredited representatives must be registered with the Executive Office of Immigration Review before appearing in Immigration Courts. In some Latino communities immigration consultants often advertise their services as *notarios públicos*, which means notaries public in English. Consumers can be confused by this title because in some countries, *notarios* have training similar to lawyers and can perform legal services. However in California, notaries public are not lawyers. *Notarios* take advantage of this confusion to demand fees for services they are not legally allowed to offer, defrauding consumers of large amounts of money in the process. That is why, under AB 1159 dated Oct. 5, 2013, immigration consultants can no longer use the term *notario* to advertise their services.

Here are a few tips to avoid fraud in hiring an immigration consultant. Some also apply to hiring an attorney.

- *Get references.* Don't hire a consultant based only on an advertisement, a phonebook listing, or a friend's recommendation. Talk to people who have used the consultant. If you find that people have lost money or paid the consultant without ever hearing back, find another consultant. Check with community groups or attorneys who specialize in immigration law to find the name of a reputable consultant.
- *Check out the consultant's background.* Once you have a name you can easily check to see if the person is registered in California. Immigration consultants are required by law to register and file a $100,000 bond with the Secretary of State. Anyone can check on an immigration consultant's bond online at **www.sos.ca.gov/business/sf/bond_search/**. Or you can call **(916) 653-4984** to check whether the person has posted the required bond and met the other requirements of Secs. 22440-22248 of the California BPC. Keep the bond number for your records. If you can't find the bond, find another consultant.
- *Ask questions.* Make sure the consultant knows how to provide the services he or she is limited to by law, i.e., translating documents for you, helping you complete forms, and submitting forms to the government.
- *Be wary if the consultant charges you for forms or requires you to pay before the work promised is done.* Most forms can be downloaded from the USCIS for free. Consultants can deceive you by charging you extra fees saying that they know someone at the USCIS who can quickly process your documents.
- *Get a written contract.* If you decide to hire a consultant, have a written contract signed and dated by the consultant. The contract should contain the consultant's full name and contact information, specify what the consultant will do, the fees you expect to pay, and other costs. It should be in English and in your language. Don't sign it unless you understand what it says. If you change your mind within 72 hours, you can cancel the contract and get all your money back. You can also cancel your contract at any time after

the initial 72 hours. Make sure the cancellation is in writing. Keep the original in a safe place and give the consultant a copy.

- *Never sign blank documents or forms that have false information.* If a consultant asks you to do this, ask for your paperwork back and find another consultant. You could be committing a crime if you sign a USCIS or other official document that contains false statements.
- *Never sign and submit any immigration document you don't understand.* Ask someone to translate the document for you if you can't read English. A consultant should not submit any documents with the USCIS if they are too complicated for you to understand or if you don't understand why you are submitting the documents.
- *Consult a person you trust before signing or paying anything.* Be suspicious of anyone who wants you to act immediately.
- *Get a dated receipt showing what you paid for and how much you paid***.** Make sure the consultant signs the receipt.
- *Keep your original documents and make copies of documents you submit to the consultant.* This includes receipts, contracts, government forms, statements, and financial records.
- *Make a complaint if you run into a problem with a consultant***.** Don't be afraid to complain. Law enforcement officials will investigate your complaint regardless of your immigration status. You can take it to the California DoJ Office of Immigrant Assistance by calling **(888) 587-0557**, filing it online at **https://oag.ca.gov/contact/consumer-complaint-against-business-or-company**, or in writing by mail to the Office of the Attorney General, Public Inquiry Unit, PO Box 944255, Sacramento, CA 94244-2550.

To avoid being a victim of an immigration scam, people with immigration problems, including young immigrants seeking help in requesting consideration in the federal government's Deferred Action for Childhood Arrivals (DACA) program which defers deportation action for two years with potential renewal and provides eligibility for employment if there is an economic necessity, should be aware of the following:

- Only immigration consultants, attorneys, notaries public, and organizations accredited by the BIA are authorized to charge existing or prospective clients fees for providing consultations, legal advice, or notary public services associated with filing an application under the federal DACA. Furthermore these individuals are prohibited from practices that amount to price gouging when a client or prospective client solicits these services, where "price gouging" means any practice that has the effect of pressuring the client or prospective client to purchase services immediately because purchasing them at a later time will result in a higher price for the same services.
- Attorneys and immigration consultants are prohibited by AB 1159 from collecting advance fees for services related to a federal immigration reform until Congress acts on it. This law also does the following:
    - Requires attorneys and immigration consultants to account for any money already accepted for immigration reform services, and either refund the money or deposit it in a client trust account.
    - Requires attorneys to give clients receiving immigration reform services written notice about where they can file a complaint about his or her services. It also increased the amount of bond that immigration consultants must carry from $50,000 to $100,000.
    - Makes it a violation of the law relating to the unauthorized practice of law for anyone who is not an attorney to literally translate from English to another language the phrases *notary public*, *notary*, *licensed*, *attorney*, *lawyer* or any other terms that imply a person is an attorney. The literal translation of the phrase *notary public* into Spanish as *notario publico* or *notario* is expressly prohibited.
- Go to **http://calbar.ca.gov/Attorneys/LawyerRegulation/FilingaComplaint.aspx** on the State Bar's website or call **(800) 843-9053** for information about filing a complaint against a lawyer licensed in California.
- You can also complain to the U.S. DoJ Executive Office for Immigration Review, which handles complaints against immigration attorneys who are licensed in any state. Call **(703) 305-0470** to get a complaint form.
- Call the State Bar at **(866) 879-4532** for information about filing a complaint against a non-lawyer.

On November 20, 2014 President Obama announced significant changes to the immigration system via executive action. Taken as a whole these changes are referred to as the Immigration Accountability Executive Actions and they present major changes to national immigration policy. This action is summarized and posted online by the USCIS at **www.uscis.gov/immigrationaction**. It was challenged by 26 states in a federal district court in Texas and a preliminary injunction against it was issued on February 16, 2015. The U. S. Court of Appeals for the Fifth Circuit in New Orleans affirmed the injunction and ordered the case back to the district court for trial. On November 10, 2015 the Justice Department announced it would ask the Supreme Court to reverse the injunction, and on January 19, 2016 the Court agreed to review the case. Then on June 23, 2016 the Court issued a one-line *per curiam* opinion affirming the lower court's judgment by an equally divided Court. Because of these decisions the action announced by the President has not been implemented and the USCIS is not accepting any requests or applications for them. Information on this website is no longer current by remains for reference purposes only. Its content has be archived.

On Sept. 5, 2017, the DHS initiated the orderly phase out of DACA. It will provide a limited, six-month window during which it will consider certain requests for DACA and applications for work authorization, under specific parameters. The details are in the memorandum from Acting DHS Secretary Elaine Duke entitled *Memorandum on Rescission of DACA*, which is on the DHS website at **www.dhs.gov/news/2017/09/05/ memorandum-rescission-daca**. After this date, individuals who have DACA will be allowed to retain both DACA and their work Employment Authorization Documents (EADs) until they expire. USCIS will adjudicate on an individual, case by case basis: properly filed pending DACA initial requests and associated applications for EADs that have been accepted as of Sept. 5, 2017; and properly filed pending DACA renewal requests and associated applications for EADs from current beneficiaries that have been accepted as of Sept. 5, 2017, and from current beneficiaries whose benefits will expire between Sept. 5, 2017 and March 5, 2018 that have been accepted as of Oct. 5, 2017. Individuals who have not submitted an application by Sept. 5, 2017 for an initial request under DACA may no longer apply. USCIS will reject all applications for initial requests received after Sept. 5, 2017. More information on the Sept. 5, 2017 DACA announcement is on the DHS website at **www.uscis.gov/daca2017**.

The State Bar website provides legal information on many immigration topics. Go to **www.lawhelpcalifornia.org**, click on Immigration, and then select from the following for the one that best matches your legal problem to get legal information and find help.

- Deportation, Removal, and Detention
- Permanent Residence/Green Cards
- Naturalization/Citizenship
- Family Petitions
- Asylum, Refugee, and Special Immigrant Juvenile
- Immigrants and Domestic Violence
- Employment Petitions
- Discrimination for Immigration Status or National Origin
- Public Benefits for Immigrants
- Citizenship through Military Service

Links to the following websites that contain information about immigration law and resources, the Dream Act, and how to get legal help on your problem can be found on the California Courts website at **www.courts.ca.gov/24641.htm**.

- CitizenshipWorks will help answer important questions about your eligibility for citizenship through naturalization. It will also help you to understand the naturalization process and prepare you for the naturalization tests.
- Immigrant Legal Resource Center has information to help you understand immigration law and your rights as an immigrant. It also tells you how to protect yourself from fraud by immigration assistants.

- National Immigration Law Center has community education material on know-your-rights alerts, eligibility for disaster assistance, affidavits of support, etc.
- Disability Rights California has information on benefits for immigrants with disabilities, etc.

Investment Opportunities

Investment pitches come by phone, postal mail, e-mail, newspaper and magazine advertisements, TV "infomercials," etc. They can also come from friends, relatives, co-workers, neighbors, and members of groups or organizations you belong to. Some may be legitimate, but many are scams designed to separate you from your money. Remember, scam artists are skilled liars. They are usually very friendly, very good at sounding like they represent legitimate businesses, and have believable answers to any questions you may ask. And they often prey on seniors, widows, fellow members of ethnic or religious groups, or cultural or community organizations whose trust they betray. The following tips will help you spot and avoid most types of investment scams:

- Don't believe claims that there is no risk. All investments, even legitimate ones, involve some risk. Never invest more than you can afford to lose.
- Be wary of promises that you will make a good return fast. Legitimate investments require time to pay off. If the offer sounds too good to be true, it probably is. Be highly suspicious of any "guaranteed' investment opportunity.
- Be suspicious of an investment in which regular, positive returns are promised regardless of the overall market conditions. Investment values tend to go up and down over time, especially those with high returns.
- Be wary of investments in gold, other precious metals, and coins. There are a variety of scams involving them.
- Never rely solely on unsolicited investment information from an e-mail or fax, especially when the sender makes extravagant claims about its future value. Be skeptical whenever you receive a stock tip. Tipsters try to get you and others to buy the stock so the price will go up and they can sell off their shares at the inflated price.
- Check the source of any message you receive because it may come from a company insider who is paid to advertise the stock.
- Don't be fooled by testimonials offered by strangers. Often these are fictitious or made by the scammers to encourage you to invest.
- Avoid investments you don't understand or for which you can't get complete information. Understand what you are investing in and how your investment will be held or managed. If you are unsure about anything, discuss the investment with your attorney, accountant, or any other licensed professional before you invest. You should also discuss it with your family and trusted friends.
- Don't be afraid to ask questions. Any legitimate business will be glad to answer them.
- Be wary of any business that does not have a street mailing address and phone number.
- Be sure to get everything in writing. Chances are you won't get what was promised otherwise.
- Read the investment's prospectus and disclosure statement carefully before you invest.
- Ask what recourse you would have if you are not satisfied with your investment or if you need to get your money out quickly. It is essential to get any warranty or refund provision in writing, and be confident that the business will honor its guarantees should that become necessary.
- Be suspicious if you don't receive a payment or have difficulty cashing out your investment.
- Be wary of salespeople who promise to "take care of everything" for you. Honest salespeople will make sure you understand the investment. They will also keep you informed about it so you can make appropriate decisions in the future.
- Don't get taken in by offers that are available right now. Don't get pushed into making a quick decision. Take time to think about it, do some research, and discuss it with others. If you are not interested, just say so; it is not impolite to simply say "no" or hang up the phone.
- Be wary of salespeople who ask you to send cash or transfer money immediately, or offer to send someone to pick it up.

- Never meet with a salesperson alone in your home.
- Don't disclose your financial situation of provide any personal information such as your SSN or credit card number until you are confident that you are dealing with a legitimate salesperson and company. Never give out personal information for "identification" purposes.
- Check the credentials and licensing of any salesperson, broker, or other person before investing. Don't deal anyone who isn't licensed. You can check out money managers, financial planners, insurance agents, and other investment advisors in California at **http://search.dre.ca.gov/integrationaspcode/**.
- Ask what state or federal agencies the salesperson's firm is regulated by and with whom is it registered. Get their phone numbers and e-mail addresses so you can contact them to verify the facts. Don't deal with salespeople who say their firm is not subject to registration or regulation.
- Don't consider investments that are not registered with the SEC or a state regulator.
- If the investment involves securities, you can go to the FINRA's website at **www.finra.org** and look up the status of brokers or brokerage firms on BrokerCheck on its Investors page. You can also get a detailed report that includes the firm's profile, history, operations, and disclosure events. The latter include arbitration awards, disciplinary actions, bankruptcies, etc. Also check with the California DBO at **www.dbo.ca.gov** or **(866) 275-2677** to verify that the company offering stock or other securities is registered, and that the investment opportunity is legitimate and legal. And you can see company's quarterly and annual reports on the SEC's website at **www.sec.gov** under Filings & Forms.
- Ask for the name of the firm your investments clear with.
- If the investment involves commodity futures, you can go to the National Futures Association's website at **www.nfa.futures.org** and look up the status of individuals or firms on its Broker/Firm Information (BASIC) page. You can also go to the Commodity Futures Trading Commission's website at **www.cftc.gov** and look up the disciplinary history of individuals or firms under Consumer Protection.
- Be wary of any individual or firm who offers to sell you commodity futures or options on commodities, particularly precious metals, foreign currency, and those with seasonal demands. These investments are very risky and anyone who claims otherwise may be breaking the law.
- If you have a self-directed IRA, i.e., one in which you can hold alternative investments such as real estate, mortgages, tax liens, precious metals, and unregistered securities, you cannot depend on the custodian to investigate and validate your investments or any financial information provided about them. Custodians are only responsible for holding and administering the assets in the IRA. And they have no responsibility for investment performance. This puts the burden on you to avoid Ponzi schemes and other frauds. For ways to avoid these dangers see the investor alert published by the SEC Office of Investor Education and Advocacy at **www.sec.gov/investor/alerts/sdira.pdf**.
- Be wary of investment offerings involving distressed real estate. Investments in properties that are bank-owned, in foreclosure, or pending short sales carry substantial risks and should be evaluated carefully. And as with other securities, interests in real estate ventures must be registered with state security regulators. For ventures in California you can check licenses on the CalBRE website at **www2.dre.ca.gov/PublicASP/pplinfo.asp**.
- Investments involving promissory notes and the persons who sell them must be registered. Check on them with the California securities regulators before investing. Unregistered notes are often covers for scams. And registered notes carry a risk that the issuer may not be able to meet its obligations.
- Don't subscribe to any offerings of equity crowdfunding by small businesses. They are illegal until the SEC, on which the Jumpstart Our Business Startup (JOBS) Act enacted in April 2012 conferred the authority to regulate them, enacts rules to guide these offerings. The SEC has not done so as of September 30, 2014. When they are enacted SEC registration will not be needed if (1) the total value of all securities sold annually does not exceed $1 million, (2) issuers abide by income and net worth thresholds for investors, and (3) issuers use registered broker-dealers or online funding portals to advertise offerings and manage the collection and distribution of investors' funds. Even then the FBI warns that some offerings may be fraudulent. Investors should be suspicious of any equity crowdfunding offers.

In selecting a financial planner, in addition to the tips listed above and other questions to ask about his or her competency, experience, education, client base, income, compensation, etc., you should do the following:

- Read the brochure entitled *What You Should Know Before Hiring a Professional Fiduciary* published by the Professional Fiduciaries Bureau (PFB) of the California Department of Consumer Affairs. It's online at **www.fiduciary.ca.gov/forms_pubs/hire_fiduciary.pdf**. It suggests that you interview at least three licensed professional fiduciaries and provides examples of interview questions to ask before becoming a client.
- Check the planner's professional credentials. These include being a Certified Financial Planner (CFP) and a Chartered Financial Analyst (CFA). For the former you can check for certification, public disciplinary history, and areas of specialization of the CFP Board's website at **www.cfp.net**. For the latter you can check the member directory on the CFA Institute's website at **www.cfainstitute.org/about/membership/directory/Pages/index.aspx** or call the Institute at **(434) 951-5262**.
- If you are investing in securities, go to the Financial Industry Regulatory Authority's website at **www.finra.org** and look up the status of brokers or brokerage firms on its BrokerCheck on its Investors page. You can also get a detailed report that includes the firm's profile, history, operations, and disclosure events. The latter include arbitration awards, disciplinary actions, bankruptcies, etc.
- Never commit to giving the planner money to invest on your first meeting. Think about the proposed investments and discuss them with people you trust. Be suspicious of planners that pressure you into investing right away.

IRS Impersonation Scams

The Treasury Inspector General for Tax Administration (TIGTA) has received reports of more than one million tax scam contacts from October 2013 to July 2016. It is also aware of more than 10,000 victims who have collectively paid $54 million as a result of tax scams since October 2013. Here are some of the most prevalent IRS impersonation tax scams.

- Scammers, using a common name with a fake IRS badge number, call and threaten those who refuse make a "tax payment" with arrest or loss of a business or driver license. The scammers may also know the last four digits of your SSN, make the IRS number appear on your Caller ID, and send bogus IRS e-mails to support their scam. Some contact people with limited English proficiency using their native language. The truth is that the IRS usually contacts people by mail first about unpaid taxes.
- Scammers call students and parents demanding payment of a fictitious tax such as a "Federal Student Tax." If the person does not comply, the scammer becomes aggressive and threatens to report the student to the police to be arrested.
- Scammers send a letter or e-mail with a fraudulent CP2000 tax bill and request the payment be sent to an IRS Processing Center at a Post Office box address. A CP2000 notice is commonly mailed to taxpayers through the United States Postal Service (USPS). It says that the income and/or payment information the IRS has on file doesn't match the information you reported on your tax return, and that this could affect your tax return and may cause an increase or decrease in your tax, or may not change it at all. Go to **www.irs.gov/individuals/understanding-your-cp2000-notice** for more information about this notice.
- Scammers call and say they need to verify a few details on your tax return in order to process it. They try to get you to give up personal information such as a SSN or financial information such as bank account or credit card numbers.

Other scammers send e-mails that appear to be official communications from the Taxpayer Advocacy Panel (TAP), a volunteer board that advises the IRS on issues affecting taxpayers, the IRS itself, or others in the tax business. These phishing schemes ask taxpayers for all kinds of personal and financial information. If you receive an e-mail that asks for personal tax information, forward it to **phishing@irs.gov** and then delete it. Don't do any of the following if you receive one of these e-mails.

- Reply
- Give out any personal or financial information
- Open any attachments or click on any links. If you click on a link you will be taken to a site designed to imitate an official site such as **www.IRS.gov**. These sites usually ask for SSNs and other personal

information that would be used to file a false tax return. These sites also may carry malware, which can infect your computer and allow criminals to access your files or track your keystrokes to gain information.

Scammers are even targeting deaf and hard of hearing individuals using Video Relay Services (VRS). They should not automatically trust calls just because they are made through VRS. VRS interpreters do not screen calls for validity. Deaf and hard of hearing taxpayers should avoid giving out personal and financial information to anyone they do not know. They should always confirm that the person requesting personal information is who they say they are, just like anyone else.

Here are a few basic tips for recognizing and avoiding a phishing e-mail scam. They are from IRS Tax Tip No. 5 dated December 6, 2016 entitled *Avoid Identity Theft: Learn How to Recognize Phishing Scam*. It's online at **www.irs.gov/uac/avoid-identity-theft-learn-how-to-recognize-phishing-scam**.

- It contains a link. Scammers often pose as the IRS, financial institutions, credit card companies, or even tax companies or software providers. They may claim they need you to update your account or ask you to change a password. The e-mail offers a link to a site that may look similar to the legitimate official website. Do not click on the link. If in doubt, go directly to the legitimate website and access your account.
- It contains an attachment. Another option for scammers is to include an attachment to the e-mail. This attachment may be infected with malware that can download malicious software onto your computer without your knowledge. If it's spyware, it can track your keystrokes to obtain information about your passwords, SSN, credit cards or other sensitive data. Do not open attachments from sources unknown to you.
- It's from a government agency. Scammers attempt to frighten people into opening e-mail links by posing as the IRS or another government agency.
- It's an "off" e-mail from a friend. Scammers also hack e-mail accounts and try to leverage the stolen e-mail addresses. You may receive an e-mail from a "friend" that just doesn't seem right. It may be missing a subject, contain an odd request, or use unnatural language. If it seems "off," avoid it and do not click on any links.
- It has a lookalike URL. The questionable e-mail may try to trick you with the URL. For example, instead of www.irs.gov, it may be a false lookalike such as www.irs.com. You can place your cursor over the text to view a pop-up of the actual URL.

In summary, the IRS will never do the following:

- Initiate contact by e-mail, text message, or social media channels to request personal or financial information, which includes PINs, passwords, or similar access information for credit cards, banks, or other financial accounts
- Call about taxes owed without first having mailed you a bill
- Call and demand immediate payment of a tax debt using a specific payment method such as a prepaid debit card, gift card, or wire transfer
- Make a robocall and leave a prerecorded, urgent message asking for a call back and threatening to issue an arrest warrant if you fail to do so
- Threaten to bring in local police or other law enforcement agency to have you arrested for not paying
- Threaten legal action such as a lawsuit
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount said to be owed
- Require you to use a specific payment method to pay your taxes, such as a prepaid debit card, gift card, or wire transfer, e.g., by a specific prepaid debit card that is linked to the Electronic Federal Tax Payment System (EFTPS) when in reality, it is controlled entirely by the scammer
- Require that you send the payment to a Post Office box address
- Ask for credit or debit card numbers over the phone
- Send a CP2000 notice as part of an e-mail, or ask for payment for taxes owed

If you get a call from someone claiming to be with the IRS asking for a payment, hang up immediately. Then if you owe Federal taxes, or think you might owe taxes, go to **www.irs.gov/uac/view-your-tax-account** to view your account and find out how much you owe, or call the IRS at **(800) 829-1040**. IRS workers can help you with your payment questions. If you don't owe taxes, don't give out any information, hang up, and contact the TIGTA at **(800) 366-4484** to report the call. Or use the IRS Impersonation Scam Reporting page at **www.treasury.gov/tigta/contact_report_scam.shtml** to report it.

Another impersonation scam that might occur starting in April 2017 is a caller claiming to be from a Private Collection Agency (PCA) that the IRS is required to use to collect, on the government's behalf, inactive tax receivables that the IRS is no longer actively working on. This scam is addressed separately next. Information on other scams involving the IRS is presented in the later the sections on Tax Debt Relief and Tax Return Fraud.

If you do get a letter or notice from the IRS by mail, which is the only way the IRS will contact you, here's the best way handle it.

- Don't panic. Simply responding will take care of most IRS letters and notices.
- Don't ignore the letter. Most IRS notices are about federal tax returns or tax accounts. Each notice deals with a specific issue and includes specific instructions on what to do. Read the letter carefully; some notices or letters require a response by a specific date.
- Respond timely. A notice may likely be about changes to a taxpayer's account, taxes owed or a payment request. Sometimes a notice may ask for more information about a specific issue or item on a tax return. A timely response could minimize additional interest and penalty charges.
- If a notice indicates a changed or corrected tax return, review the information and compare it with your original return. If the taxpayer agrees, they should note the corrections on their copy of the tax return for their records. There is usually no need to reply to a notice unless specifically instructed to do so, or to make a payment.
- Taxpayers must respond to a notice they do not agree with. They should mail a letter explaining why they disagree to the address on the contact stub at the bottom of the notice. Include information and documents for the IRS to consider and allow at least 30 days for a response.
- There is no need to call the IRS or make an appointment at a taxpayer assistance center for most notices. If a call seems necessary, use the phone number in the upper right-hand corner of the notice. Be sure to have a copy of the related tax return and notice when calling.
- Always keep copies of any letters and notices you receive with your tax records.
- For more information on responding to an IRS letter or notice, go to **www.irs.gov/individuals/understanding-your-irs-notice-or-letter** on the IRS website. And see Publication 594 on the IRS collection process at **www.irs.gov/pub/irs-pdf/p594.pdf**.

IRS PCA Impersonation

Another IRS impersonation scam that might occur starting in April 2017 is a caller claiming to be from a Private Collection Agency (PCA). The IRS was required by Sec. 32102 of the Fixing America's Surface Transportation (FAST) Act to use them to collect, on the government's behalf, inactive tax receivables that the IRS is no longer actively working on. This Act was signed into law on December 4, 2015. It amended Sec. 6306 of the 1986 Internal Revenue Code. In Newswire IR-2016-125 dated Sept. 26, 2016 that the IRS announced that the following four contractors were selected for this new private debt collection program: CBE Group of Cedar Falls IA, Conserve of Fairport NY, Performant of Livermore CA, and Pioneer of Horseheads NY. More information on PCAs and a list of taxpayer accounts that will not be assigned to them can be found on the IRS website at **www.irs.gov/businesses/small-businesses-self-employed/private-debt-collection**.

To help taxpayers avoid confusion and understand their rights and tax responsibilities, particularly in light of continual phone scams where callers impersonate IRS agents and request immediate payment, the IRS will

send each taxpayer and their representative a letter informing them that their account is being transferred to a PCA. It will also give them the name and contact information for the PCA and a unique taxpayer authentication number that will enable them to verify that the debt collector who contacts them is authorized to collect the debt under contract with the IRS. This mailing will also include a copy of IRS Publication 4518 entitled *What You Can Expect when the IRS Assigns Your Account to a Private Collection Agency*.

The designated PCA will then send you a second, separate letter confirming assignment of your tax account. It will include the same unique taxpayer authentication number that is on the letter sent to you from the IRS. The PCA employee who contacts you will use the unique number to verify that it is authorized to proceed to collect your debt. Keep both letters in a safe place for future reference. Information in these letters will help taxpayers identify the tax amount owed and assure them that that future PCA calls they may receive are legitimate. Employees of the PCAs will identify themselves as contractors of the IRS collecting taxes. They must follow the provisions of the FDCPA and like IRS employees, must be courteous and respect taxpayer rights. Taxpayers should not be surprised by all of this because they have unpaid tax debts going back several years and have been contacted by the IRS about them previously. You should all the IRS directly if you have any questions about the assignment of your account to a PCA, the use of your authentication number, or the identity of the person who contacts you

The PCAs are authorized to discuss payment options, including setting up payment agreements, but as with cases assigned to IRS employees, any tax payment must be made, either electronically or by check, to the IRS. A payment should never be sent to the PCA or anyone other than the IRS or the U.S. Department of the Treasury. Checks should only be made payable to the United States Treasury. To find out more about available payment options, visit **www.irs.gov/payments**. PCAs are not authorized to take enforcement actions against taxpayers. Only the IRS can do that, e.g., filing a notice of Federal Tax Lien or issuing a levy.

Like the IRS, PCAs will never do the following:

- Initiate contact by e-mail, text message, or social media channels to request personal or financial information, which includes PINs, passwords, or similar access information for credit cards, banks, or other financial accounts
- Call about taxes owed without first having mailed you a bill
- Call and demand immediate payment of a tax debt using a specific payment method such as a prepaid debit card, gift card, or wire transfer
- Make a robocall and leave a prerecorded, urgent message asking for a call back and threatening to issue an arrest warrant if you fail to do so
- Threaten to bring in local police or other law enforcement agency to have you arrested for not paying
- Threaten legal action such as a lawsuit
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount said to be owed
- Require you to use a specific payment method to pay your taxes, such as a prepaid debit card, gift card, or wire transfer, e.g., by a specific prepaid debit card that is linked to the Electronic Federal Tax Payment System (EFTPS) when in reality, it is controlled entirely by the scammer
- Require that you send the payment to a Post Office box address
- Ask for credit or debit card numbers over the phone
- Send a CP2000 notice as part of an e-mail, or ask for payment for taxes owed
- Visit a taxpayer at their home or business

If you get a call from someone claiming to be with a PCA asking for a payment, hang up immediately. If you owe Federal taxes, or think you might owe taxes, call the IRS at **(800) 829-1040** to get help with your payment questions. If you don't owe taxes, contact the TIGTA at **(800) 366-4484** to report the call. Or use the IRS Impersonation Scam Reporting page at **www.treasury.gov/tigta/contact_report_scam.shtml** to report it.

IRS Visits

With continuing phone and in-person scams taking place across the country, the IRS reminds taxpayers that some IRS employees do make official, sometimes unannounced, visits to taxpayers as part of their routine casework. Taxpayers should keep in mind the reasons these visits occur and understand how to verify if it is actually the IRS knocking at their door. More information about this is on the IRS visits on its website at **www.irs.gov/uac/newsroom/how-to-know-it-s-really-the-irs-calling-or-knocking-on-your-door**. Visits typically fall into the following three categories:

- IRS revenue officers routinely make unannounced visits to a taxpayer's home or place of business to discuss overdue taxes, delinquent tax returns or employment tax payments. Revenue officers are IRS civil enforcement employees whose role involves education, investigation, and when necessary, appropriate enforcement. They will request payment of taxes owed by the taxpayer; however, payment will never be requested to a source other than the U. S. Department of the Treasury.
- IRS revenue agents will sometimes visit a taxpayer who is being audited. That taxpayer would have first been notified by mail about the audit and set an agreed-upon appointment time with the revenue agent. Also, after mailing an initial appointment letter to a taxpayer, an auditor may call to confirm and discuss items pertaining to the scheduled audit appointment.
- IRS criminal investigators may visit a taxpayer's home or place of business unannounced while conducting an investigation. They are federal law enforcement agents and will not demand any sort of payment.

If an IRS representative visits you, he or she will always carry two forms of official credentials: a pocket commission and a Personal Identity Verification Credential (PIV). Pocket commissions describe the specific authority and responsibilities of the authorized holder. The PIV is a government-wide standard for secure and reliable forms of identification for federal employees and contractors. It was developed under Homeland Security Presidential Directive12 (HSPD-12) and designed to enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification. Both forms of ID have serial numbers. Taxpayers can ask to see both. You can find out more about this card at **www.fedidcard.gov**. Criminal investigators also have a badge and law enforcement credentials.

Job Scams

Persons looking for jobs need to be aware of various scams. In one scammers ask for upfront money or personal information for help in finding a job. They keep the money and use the personal information for identity theft. The following red flags warn you of this job scam:

- The employer or a placement agency asks for upfront money. Scammers will say upfront money is needed for background checks or expenses for placing you in jobs that don't exist. Employers or placement agencies shouldn't ask you to pay for the promise of a job.
- The employer or agency asks for personal information before you get the job. This is an attempt to get your SSN and bank account numbers, which can be sold to identity thieves or companies with products or career training programs they could sell.
- The employer requires you to get a credit report from a recommended website. This is an attempt to get personal financial information or sell you credit monitoring services.
- The ad is for "previously undisclosed" federal government jobs. Information about available federal jobs is free. All federal jobs are announced to the public on **www.usajobs.gov**. Don't believe anyone who promises you a federal job.
- Employer or agency e-mails are full of grammatical and spelling errors. They usually come from scammers outside the U.S. where English is not their first language.
- The salary and benefits offered seem too good to be true. Phony employers will promise high salaries and good benefits for little work with no experience necessary.
- The employer offers the opportunity to become rich without leaving home. While many legitimate businesses allow employees to work from home, many scammers try to take advantage of seniors, stay-

at-home moms, students, injured or handicapped people, and those otherwise unemployed. They often require an upfront investment in office supplies and other materials and then fail to deliver the salaries promised. Legitimate businesses that offer work-at-home arrangements typically pay from $8 to$15 an hour. These jobs involve low risks and have low rewards.

- The employer asks you to receive packages at your home or business and mail them to someone else, usually out of the country. These packages contain thingse bought with stolen credit cards. If you reship them you become part of a smuggling operation and can be arrested and charged with mail fraud, etc.
- The employer sends you a check that might be an advance for expenses and asks you to wire back any amount not used. The check will be fraudulent. If you cash it your bank will ask you to pay it back when the check does not clear the bank is written on.
- The employer wants you to travel to Mexico or someplace else outside the U.S. for an interview, tour, or something else.

In another job scam, FBI Public Service Announcement I-011817-PSA at **www.ic3.gov/media/2017/170118.aspx** dated January 18, 2017 warned college students about scammers who continue to advertise phony job opportunities on college employment websites or sent e-mails to student's school accounts recruiting them for fictitious administrative positions. Students who respond are sent counterfeit checks to be deposited in their personal checking accounts and then withdraw funds and send a portion via wire transfer to another individual or a "vendor" purportedly for equipment, materials, or software necessary for the job. Subsequently, the checks are confirmed to be fraudulent by the bank and the students suffer the following consequences.

- Their bank account may be closed due to fraudulent activity and a report could be filed by the bank with a credit bureau or law enforcement agency.
- They are responsible for reimbursing the bank the amount of the counterfeit checks.
- Their credit record could adversely affected.
- Any personal information given to the "employer" leaves them vulnerable to identity theft.

To avoid becoming a victim of these scams, students should never accept a job that requires depositing checks into their accounts or wiring money to other individuals or accounts. And because many scammers who send these messages are not native English speakers, look for incorrect grammar, capitalization, and tenses in the e-mails. Students should also forward suspicious e-mails to their college's IT personnel, report them to the FBI, and tell their friends to be on the lookout for the scam.

Before dealing with any company or placement agency, do some research on it. First find out where it is located. Don't have anything to do with a company that has a Post Office box for an address. Then do a search of the records in the state in which it is incorporated or registered to verify any information provided. And check it out with the BBB at **www.bbb.org/sdoc**. Also do in Internet search on it with words like "review," "scam," or "complaints."

In considering an employment agency, get a copy of the contract and read it carefully before your decide to deal with it. Make sure all promises are in writing, including those about refunds if the agency doesn't find a job for you or give you any good leads. If the agency doesn't answer all your questions, or gives you confusing answers, don't deal with it. Remember, job information is free, you shouldn't pay for it. A website sponsored by the U.S. Department of Labor, **www.CareerOneStop.org**, lists hundreds of thousands of jobs. It also has links to employment and training programs in each state, including ones for people with disabilities, older workers, veterans, welfare recipients, and young people. You can also search for jobs on the California Employment Development Department website at **www.caljobs.ca.gov/vosnet/Default.aspx**.

Land Investment Fraud

Here are some things to do to avoid being scammed in land investments.

- Never buy land unseen.
- Visit the records office in the city or county where the land is located and check the history of the land. This information is available to the public.
- Make sure the company or person selling the land is licensed and their venture is registered with state security regulators. For ventures in California you can check licenses on the CalBRE website at **www2.dre.ca.gov/PublicASP/pplinfo.asp**. You can also check the company or person with the BBB.
- Don't take the word of salespeople regarding projected population growth where the land is located. Check documents published by government agencies that do this, e.g., the San Diego Association of Governments (SANDAG).
- Ask about the downside of any investment.
- Never make verbal agreements.
- Never sign blank pages where information can be added later.
- Get a real estate attorney to review any paperwork.
- And as in other investments: never make agreements under pressure, walk away from any deal that must be made immediately, be wary of promises of guaranteed rates of return, be wary of anyone contacting you to invest, and use your common sense, if the deal sounds too good to be true it probably is.

Suspected scams should be reported to the San Diego County District Attorney's Real Estate Fraud Program. Call its complaint line at **(619) 531-3552** to request a complaint form. Write or type a summary of your complaint and attach it to the complaint form. Your complaint cannot be reviewed without a complete concise statement of the facts. At a minimum, the following information should be included in your statement:

- What happened chronologically. Be specific. Tag as exhibits any supporting documents and refer to those exhibits in your narrative. Documentary evidence is especially important. Include photocopies of all documents and materials (contracts, agreements, certificates, notes, deeds, correspondences, front and back of involved checks, escrow and/or loan documents, etc.) you wish to be reviewed. Retain the originals for your records.
- Who you think the person(s) or company that is responsible for the loss, conversion(s), or fraudulent act. State why you conclude that.
- Where (address, city, and state) the incident, conversions, or act(s) took place. Include property address(es) involved in the fraudulent transaction(s).
- When and how you first became aware that you may have been defrauded. If individual(s) or a company is named in your complaint, please list exact dates of contact. If someone else made you aware of the potential crime, please include the person's name(s), address(es), and telephone number(s).
- How you know the representations were false, or how you know money was misused.
- What your actual financial loss is, if known.

Landlord Impersonation

In this scam, which has become more frequent as the number of vacant and foreclosed homes increases, a person pretending to be the property owner rents a home to a prospective tenant and asks for first- and last-month's rent and a security deposit in cash. The rents are typically much lower than those of similar homes in the neighborhood. All this money will be lost and the "tenants" can be evicted when the real property owner shows up. Before renting, prospective tenants should call the San Diego County Assessor's Office to make sure the person renting the property is the real owner. You can call its public information number, **(619) 236-3771**, on weekdays from 8 a.m. to 4 p.m. to get the property owner's name.

The Federal Home Loan Mortgage Corporation, known as Freddie Mac, which owns foreclosed homes, suggests that prospective renters do the following to avoid being scammed.

- Check to make sure the home is not already listed for sale. You can Google the address and drive by to see if there are signs posted. You can also check Freddie Mac's foreclosure sales listings at **www.homesteps.com**.
- If you discover the home is already listed for sale, notify the listing agent of the attempted scam. And report it to the San Diego County District Attorney's Real Estate Fraud Program. Call its complaint line at **(619) 531-3552** to request a complaint form. Write or type a summary of your complaint and attach it to the complaint form. Your complaint cannot be reviewed without a complete concise statement of the facts.
- Never submit an online lease application until you have verified that the rental is legitimate. Otherwise you risk losing personal financial information.

Mail Fraud

Mail fraud is a scheme that uses the mail to get money or something of value from you by offering a product, service, or investment opportunity that does not live up to its claims. It is often an element in many of the scams covered in this section, including those that deal with charities, credit repair, fraudulent checks, investment opportunities, job offers, insurance sales, prize notification and lotteries, and unscrupulous contractors. Some others that are addressed by the U.S. Postal Inspection Service (USPIS) in its *Guide to Preventing Mail Fraud* dated June 2010 are summarized below.

- You get a letter saying you have won a free vacation and just need to call to make reservations. When you call you will find that the dates you prefer aren't available and you need to pay a service charge or purchase a membership in a travel club to make reservations on other dates. If you do that you'll lose your money, and if you pay by credit card you'll also lose your identity.
- You get a letter in an envelope that appears in all respects to come from a government agency. The letter inside requests a donation to a political cause. This is legal if the letter comes from an organization with a legitimate government connection. If the organization does not have that connection, it is legal only if the envelope and letter have a statement that disclaims a connection, approval, or endorsement of a government agency, or if the material in the envelope is contained in a publication you purchased or requested. Otherwise, this is a fraud.
- You get an invoice stating that you owe money for some goods or services that you received. Don't pay unless you verify that you actually ordered and received them. Con artists mail solicitations disguised as invoices knowing that some unsuspecting people will not remember what they ordered and received and pay the amount "owed."
- You get a chain letter guaranteeing you'll receive a lot of money from one small investment. For example, it might say that all you have to do is send $10 to everyone on the list, put your name on the bottom of the list, and mail the list to 10 friends. Don't waste your money. Chain letters don't work. And if you mail them you could be committing a federal crime. The same law that prohibits lotteries also applies to chain letters.
- Beware of offers of miracle drugs and cures for arthritis, obesity, baldness, sexual dysfunction, and other common problems. The various gadgets and gimmicks advertised are not tested for effectiveness by competent medical authorities and may actually be dangerous to use. Protect your health and pocketbook. Consult your family doctor before buying any advertised medicines.
- You receive letter saying that you have been named as an heir in an estate that is currently being settled, and all you have to do is mail a small fee to find out what your share is. This is a scam. An executor will not request a fee for telling you about an inheritance.
- Beware of mail solicitations that offer to obtain government and other services for you for a fee. Many of these services are available free of charge. They include tax refunds, property tax exemptions, child support collection assistance, loan modification, immigration forms and information, etc. Contact the

federal, state, and local agencies that provide these services for information and assistance is obtaining forms and information at no cost.

- Many distributorships and franchises are legitimate and can be profitable for people willing to invest a substantial amount of money. However, some promoters advertise fraudulent opportunities and keep the investors' money. Beware of promoters who promise unrealistic profits, seem more interested in taking your money than the services being offered, and are reluctant to let you contact current franchisees.
- You get some merchandise in the mail that you did not order. The sender may try to get you to pay for it. By law, unsolicited merchandise is yours to keep. You don't have to pay for it even if the sender follows up with a phone call or visit. If you haven't opened the package and don't want it you can mark it RETURN TO SENDER. The U.S. Postal Service will send it back at no charge to you. If you open the package and decide you don't want what's in it, just throw the contents away.

If you believe you've been victimized by or suspect mail fraud, contact the USPIS by calling **(877) 876-2455** or reporting it online at **www.postalinspectors.uspis.gov**.

Marijuana Stocks

By May 2014, with medical marijuana legal in almost 20 states, and recreational use of the drug recently legalized in two states, the cannabis business was getting a lot of attention. As media coverage increased, so did investor interest in stocks of marijuana-related companies. In some cases share volume increased dramatically and prices became quite volatile. Then the SEC issued an alert and accompanying trading suspensions for numerous companies that claim their operations relate to the marijuana industry. And FINRA reissued its August 2013 warning about the potential for fraud in this area and the risks of investing in thinly-traded companies about which little is known.

Stock scammers typically publish optimistic and potentially false and misleading information designed to create unwarranted demand for shares of a small company with little or no history of financial success. Once share prices and volumes reach a peak they will sell their shares at a profit and leave investors with worthless stock. This called "pump and dump." Here are some of the tips FINRA has published to help people avoid these scams.

- Ask why a total stranger would contact you about a really great investment opportunity? The answer is that there is likely no true opportunity. In many scams those who promote the stock are corporate insiders, paid promoters, or substantial shareholders who would profit handsomely if the company's stock price goes up.
- It's easy for companies or their promoters to make exaggerated claims about lucrative contracts and the company's revenue, profits, or future stock price. Be skeptical about companies that issue a barrage of press releases and promotions in a short period of time, especially if they only focus on a stock's upside with no mention of risk.
- Search the names of key corporate officers and major stakeholders, as well as the company itself. Look for recent indictments or convictions, time served in prison, investigative articles, corporate name changes, or any other information that raises red flags.
- Ask where the stock is traded. Beware of stocks that are traded over the counter (OTC). Note that there are no minimum quantitative standards that a company must meet to have its securities quoted in the OTC market. And many stocks quoted there don't have a liquid market. They are traded infrequently and can move up or down in price substantially from one trade to the next. This may make it difficult to sell your stock at a later date.
- Read the company's SEC filings, if available, to verify any information you have heard about the company. Check the SEC's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database to find out whether the company files with the SEC; most public companies do. Remember that just because a company has registered its securities or has filed reports with the SEC does not mean it will be a good investment for

you. Also be aware that not all financial information filed with the SEC or published elsewhere is independently audited.

- Be wary of frequent changes to a company's name or business focus. Name changes and the potential for stock fraud often go hand in hand. Name changes can turn up in company press releases, Internet searches, and if the company files periodic reports, in the SEC's EDGAR database.
- Check the credentials and licensing of the person selling the stock before investing. Don't deal anyone who isn't licensed. You can check out money managers, financial planners, insurance agents, and other investment advisors in California at **http://search.dre.ca.gov/integrationaspcode/**. Then check that the person's firm is registered with FINRA, the SEC, and the California DBO. Go to FINRA's website at **www.finra.org** and look up the status of brokers or brokerage firms on BrokerCheck on its Investors page. You can also get a detailed report that includes the firm's profile, history, operations, and disclosure events. The latter include arbitration awards, disciplinary actions, bankruptcies, etc. You can see company's quarterly and annual reports on the SEC's website at **www.sec.gov** under Filings & Forms. And go to the California DBO's website at **www.dbo.ca.gov** or call **(866) 275-2677** to verify that the company offering stock or other securities is registered, and that the investment opportunity is legitimate and legal. Also verify the caller's identity using the phone number on the firm's website or in a publicly available telephone directory.

Medicare Enrollment Fraud

Seniors should be on the lookout for Medicare scams especially during the open enrollment period that runs from October 15 to December 7 each year. The scammers will try to obtain your personal information or sell you a plan that's not the best fit your needs. You can protect yourself by doing the following:

- Don't give out personal information to anyone claiming to be from Medicare, or anywhere else. Medicare already has your personal information. It will not contact you by phone or e-mail, or visit your home. However, it is all right to provide Medicare information if you have initiated a call to Medicare for assistance, or to Medicare-plan provider when you choose to enroll in a plan.
- Be wary of brokers who try to pressure you into enrolling in a specific plan. Medicare-plan providers aren't allowed to make cold calls or come to your door unless they are invited. And don't believe claims that a plan is "Medicare Endorsed" or that you will lose benefits unless you enroll in a specific plan.
- Research and verify plans with Medicare by calling **(800) 633-4223** or going to **www.medicare.gov**.

Seniors should also be on guard for scammers who say they need new policies under the Affordable Care Act (ACA), commonly called Obamacare, which has open enrollments between November 15 and February 15 of the following year. The ACA does not affect persons 65 and over who have Medicare. No one from Medicare will call about the ACA. And new Medicare cards are not needed.

Medicare and Medi-Cal Services Fraud

It is estimated that Medicare fraud costs the government $60 to $90 billion per year in false or questionable claims. You can help stop this fraud by reporting suspicious activities to the Inspector General of the U. S. Department of Health & Human Services by calling **(800) 447-8477** or reporting it online at **http://oig.hhs.gov/fraud/report-fraud/index.asp**. If the activity turns out to be a fraud you may be eligible for a reward of up to $1,000. For more information on stopping Medicare fraud go to **www.stopmedicarefraud.gov**. If you suspect Medi-Cal fraud, call the California Department of Health Care Services Medi-Cal Fraud Hotline at **(800) 822-6222**.

Watch out for these common fraud schemes in which someone does the following:

- Says you qualify for some health care equipment like a motorized scooter and it won't cost you anything. All you need to do is provide your Medicare number so he or she can contact your doctor and get the order approved.

- Says he or she knows how to get Medicare to pay for some health care item or service you might want.
- Approaches you in a parking lot, shopping center, or other public area and offers free services, groceries, transportation, or other items in exchange for your Medicare number.
- Calls you on the phone, claims to be conducting a health survey, and asks for your Medicare number and medical history.
- Calls you on the phone, says her or she is from Medicare or Social Security, and asks for personal medical information or tries to sell you some health care items or services.
- Comes to your door and tries to sell you some health care service. Some may say that they represent Medicare and that Medicare wants you to have the service. Medicare doesn't call or visit and try to sell or give you anything.
- Offers you money to disenroll from your current Medicare plan and enroll in another plan.
- Offers you money to use a doctor you don't know to get some health services you have never heard about.

Be suspicious of doctors or insurance plans that do the following:

- Advertise "free" consultations to people with Medicare.
- Claim they represent Medicare or a branch of the Federal government.
- Use pressure or scare tactics to sell you high-priced medical services or diagnostic tests.
- Bill Medicare for services you didn't get.
- Use telephone calls and door-to-door selling as marketing tools.
- Offer non-medical transportation or housekeeping as Medicare-approved services.
- Put the wrong diagnosis on the claim so Medicare will pay for it.
- Bill home health services for patients who aren't confined to their home, or for Medicare patients who still drive a car.
- Bill Medicare for medical equipment for people in nursing homes.
- Ask you to contact your doctor and ask for a service or supplies that you don't need.
- Bill Medicare for a power wheelchair or scooter when you don't meet Medicare's qualifications.
- Offer you a kickback or some other type of bribe to bring your medical needs to a specific clinic or provider. This is illegal.
- Offer you a discount on your deductible or regularly waive payments for services you don't need.
- Tell you that the more tests you take, the cheaper they become.
- Bill Medicare for tests you receive as a hospital inpatient or within 72 hours of discharge.
- Bill social activities as psychotherapy, or provide therapies you cannot benefit from or equipment you cannot use.

There is a wide variety of health care scams. Without going into detail about each one, here are some ways for you to protect your health care benefits.

- Treat your Medicare number like your SSN. Never give it to anyone who calls on the phone. Scammers will try to get it so they can file claims in your name. And never give it to anyone who says they are from Medicare or any other branch of the government. Medicare will never call and ask for your number, it already has it. And don't carry your card unless you will need it that day.
- Never give out any Medicare claim information over the phone. Any legitimate caller will already have this information.
- Never let anyone borrow or pay to use your Medicare card. That's illegal and not worth it.
- Never allow people to fill in information on a form after you've signed it. They may be adding things you did not receive or falsify other information in order to receive more money than they are due.
- Be aware that anyone who works in a clinic can commit Medicare fraud. Be suspicious of anyone who tries to get your personal information. They may use it to file fraudulent claims in your name.
- Don't accept offers of money or free food or gifts for medical care. Watch out for incentives like "it's free" or "we know how to bill Medicare."

- Keep a record of your medical bills and doctor visits, tests, procedures you had and products and equipment you received. Save your receipts and statements. Use them for checking your monthly Medicare Summary Notices (MSNs) for mistakes and charges you did not incur. Look for services or products you didn't receive, billing twice for the same thing, or bills for services not ordered by your doctors. You can view your Medicare account records online at **www.MyMedicare.gov**.
- Contact your health care provider about any errors or unusual or questionable charges. They may just be mistakes. Ask for an itemized statement if you don't have one. If your complaint is not resolved to your satisfaction, report it to Medicare at **(800) 633-4227**.
- If there is any health service or product listed in your MSNs that you did not receive or have prescribed for you, call the Inspector General of the U. S. Department of Health & Human Services at **(800) 447-8477** or report it online at **http://oig.hhs.gov/fraud/report-fraud/index.asp**. Unscrupulous clinics, physician, and durable medical equipment providers may be billing you for goods or services you never received. This affects your ability to obtain those items when you really need them.
- Check your credit reports for any unpaid bills for health services or products that you didn't receive.
- Challenge any collection notices for health services or products you didn't receive.

Moving Scams

While most moves are made without incident, the number of complaints against rogue moving companies has increased steadily over the past decade. So you need to be aware of the ways you can be scammed and learn how to avoid them. Here are some things to watch out for in selecting a moving company.

- The company does not have a local address or contact person.
- Its phone is answered with a generic "movers" or "moving company" and not a company name.
- Its office and warehouse are in poor condition or nonexistent.
- It demands an advance payment or deposit before the move.
- It doesn't conduct an inspection and inventory of the items to be moved.
- It quotes a low price over the phone or by e-mail.
- It doesn't give you a written price estimate.
- It claims that all goods are covered by its insurance.
- For interstate moves it does not give you a copy of *Your Rights and Responsibilities When You Move*, a booklet Federal regulations require movers to give to their customers in the planning stages of interstate moves.
- For moves within California it does not give you a copy of *Important Information for Persons Moving Household Goods*, a booklet California regulations require movers to give to their customers in the planning stages of moves within California.

The following might occur on moving day if you happen to select a rogue mover.

- A rental truck arrives rather than a company-owned truck with the company name on it.
- The truck driver or move foreman will try to get you to sign blank documents before beginning to load your goods.
- You are told the load is larger than originally estimated and the actual price will be higher.
- You are told you must pay in full before your goods are loaded.

You should do the following to avoid moving scams.

- Get a list of reliable movers from the American Moving & Storage Association at **http://209.166.141.21/4dcgi/amsa/atoz/moversatoz.html?menukey=1** or the California Moving & Storage Association at **http://directory.thecmsa.org/directory/mover/mover_member_search.asp** if your friends or family don't have recommendations
- Get written estimates from several movers, not brokers. Each must conduct a visual inspection of the items to be moved for the estimate to be legal and enforceable. Federal law requires one of two kinds of

moving contracts. A non-binding estimate means the company cannot require payment of more than 10 percent above the original estimate. A binding estimate or "not to exceed" contract is supposed to be a guaranteed price for the move and all specified extras and services. An extra fee can be charged if additional services are requested and detailed in a contract change order.

- Get everything in writing. The estimate and all extra fees should be in it as well as your pickup and delivery dates. Read your contract carefully and make sure that all your belongings are listed. You can't file a claim for something that's lost if it doesn't appear on the inventory list. And never sign a blank contract form.
- Make sure the company is licensed and insured. For interstate movers, go to the Federal Motor Carrier Safety Administration's Household Goods Program page at **https://ai.volpe.dot.gov/hhg/search.asp** to search for company USDOT and MC numbers, address and phone numbers, safety rating, complaint history, insurance data, etc. For California movers, go to the California PUC's Transportation Carrier Lookup page at **http://delaps1.cpuc.ca.gov/public_cpuc/f?p=203:35:17590449600511::NO::P35_CARRIER_TYPE:MTR** to get carrier license and insurance details.
- Read and understand the booklets that movers are required to give you. They are *Your Rights and Responsibilities When You Move* for interstate moves and *Important Information for Persons Moving Household Goods* for moves within California. All moving companies are required to assume liability for the value of the goods that they transport. In choosing between two different levels of liability offered you need to understand the different charges and the amount of protection provided by each level. They are explained in these booklets. Be sure to read this information carefully and follow the instructions provided to declare a value on your shipment. Or you can buy optional insurance that is regulated under state law. The mover's representative can advise you of the availability of liability insurance and the cost.
- Check the company's rating and complaint history on the Better Business Bureau (BBB) of San Diego, Orange, and Imperial Counties' website at **www.bbb.org/sdoc**. If the company is not accredited and rated, ask for three references of people in your area who were moved in the past three months. Then call them and ask about their experience with the company.
- Refuse to pay in advance. Pay when the move is completed and your goods are delivered. Then pay with a credit card. That will make it easier to deal with any fraud that might occur.

Go to **www.fmcsa.dot.gov/protect-your-move** for more information on protecting yourself from moving fraud, spotting rogue movers, choosing a reputable mover, answers to questions about how to protect yourself from fraud, your rights and responsibilities, understanding valuation and insurance options, etc.

Obamacare

The Affordable Care Act (ACA), signed into law in March 2010 and commonly called Obamacare, like any new federal program, has provided many opportunities for scammers to prey on consumers for information to commit identity theft, charge your existing credit cards, debit your checking account, write fraudulent checks, take out loans in your name, and open a new credit card, checking, or savings accounts.

Here are a few tips for avoiding these scams.

- There are no cards for Obamacare. People selling cards are trying to steal money or personal information. There are also no "National Health Care" cards. And there is no such thing as "Obamacare insurance."
- You don't have to pay for help or information about the new law**.** Help with enrollment will be available from Covered California by calling **(800) 300-1506** or requesting assistance on its website at **www.coveredca.com**.
- Don't enroll for health care coverage with anyone who contacts you and says he or she is from the government. No legitimate government representative will try to sell insurance to you.
- Beware "insurance" sellers who use aggressive sales tactics, e.g., saying that you will go to jail if you don't enroll now, or you need to buy additional death panel insurance to cover the costs of treatment denied by the death panel.

- Don't pay cash for any coverage.
- Don't sign anything you don't understand. Get a second opinion from someone you trust.
- Don't give out your personal information to anyone you don't know, especially over the phone**.**
- Don't use an Internet search to get information about Obamacare. And don't click on any links to health insurance exchanges that you might get in an e-mail or find in an Internet search. Many fake websites can show up. Go directly to the official websites. The official federal website is **www.HealthCare.gov**. The official one for California is **www.coveredca.com**.
- Call Covered California or e-mail its Office of Consumer Protection at **consumerprotection@covered.ca.gov** to report any fraud connected with enrollment in Covered California. It will investigate, follow up, and work with appropriate law enforcement agencies on a case-by-case basis.

Seniors should beware of scammers who ask for personal information and say they need new policies. Obamacare does not affect persons over 65 who have Medicare. No one from the government will call about the Obamacare. And new Medicare cards are not needed. Persons over 65 on Medicare do not have to do anything under Obamacare. They should call the Health Insurance Counseling and Advocacy Program (HICAP) at **(800) 434-0222** with any questions about Medicare. And they can call the Senior Medicare Patrol at **(855) 613-7080** regarding possible fraud.

Pension Advances

Pension advances are loans against defined-benefit pensions, such as those for military and other government retirees. They offer retirees a chance to convert future pension checks into present cash. Retirees are required to pay off the loan from their pension checks in a set period of time, usually five or 10 years. Furthermore, to qualify for some loans, borrowers are required to take out a life insurance policy that names the lender as the sole beneficiary. Or they are required to set up a separate bank account, controlled by the lender, into which the retiree's pension checks are deposited. In doing so, the lenders circumvent usury laws. They claim the advances are not loans that are covered by federal and state regulations.

In an undercover investigation of 19 companies that offered pension advances, the Government Accountability Office (GAO) in report GAO-14-420 entitled *Pension Advance Transactions: Questionable Business Practices Identified* and published in June 2014, received offers from six of these companies. It found that they did not compare favorably with other financial products or offerings such as loans and lump-sum options through pension plans. For example, the effective interest rates offered were 27 to 46 percent, which were two to three times higher than the legal state limits for various types of personal credit. The GAO also found questionable practices related to the disclosure of rates or fees, and certain unfavorable terms of agreements. Another review of more than two dozen contracts for pension-based loans found that after factoring in various fees the effective interest rates ranged from 27 percent to 106 percent. And information about these fees was not disclosed in the ads or in the contracts themselves.

You can avoid becoming a victim of this scam and getting deep in debt by doing the following.

- Do not enter into any agreement with a company that offers pension advances.
- If you need present cash investigate and consider other alternatives, including borrowing from a regulated financial organization.

Post-Foreclosure Solicitations

Tenants in foreclosed homes and former homeowners who remain in them may be solicited by persons or companies promising to help them stay in the home and avoid eviction. The dangers are that the solicitor is not licensed, doesn't know the law, is behaving unethically, or takes an advance fee and fails to provide any services. Solicitations by attorneys cannot be threatening, raise false hopes or guarantee the result of the representation, or be made in person or by phone. And if by mail, they must bear the word "Advertisement."

Real estate agents must act fairly and honestly with respect to the transaction. Misrepresentations, harassment, failure to disclose material information or advise the person in the home of his or her rights with respect to eviction as a result of foreclosure, or negligence could possibly lead to disciplinary action.

Any advice you get should be based on the notice requirements of the California Code of Civil Procedure (CCP) Secs. 1161a, 1161b, and 1161c, the Tenants' Right to Know Regulations of the SDMC Secs. 98.0701 *et seq*, and the Federal Protecting Tenants at Foreclosure Act of 2009, which is part of the Helping Families Save Their Homes Act of 2009 (Public Law 111-22, approved May 20, 2009). This act requires that tenants living in foreclosed residential properties be given notice to vacate at least 90 days in advance of the date the purchaser wants the property vacated. Except where the purchaser will occupy the property as his or her primary residence, the term of any bona fide lease remains in effect. These protections also apply to tenants in Section 8 housing. Those tenants in San Diego with any questions about solicitations should call their assigned Housing Assistant.

Because law dealing with post-foreclosure eviction is very complex, you should talk to an attorney as soon as possible to protect your rights if you receive an eviction notice. Responses must be made within five days of receiving court papers. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups on the California Legal Services website at **www.lawhelpcalifornia.org**, the California Courts Online Self-Help Center at **www.courtinfo.ca.gov/selfhelp**, or by contacting your local court or county bar association.

Solicitations are legal as long as the solicitor is licensed. You can check real estate licenses on the CalBRE website at **www2.dre.ca.gov/PublicASP/pplinfo.asp**. You should also check that a company is licensed to work in the City of San Diego, i.e., that it has a Business Tax Certificate. You can check this in the business listings on Master Business Listings page of the City's website at **www.sandiego.gov/treasurer/taxesfees/btax/nblactive.shtml**. For legal services you need a licensed attorney. Real estate agents or companies cannot offer legal advice. You can check whether a person is a licensed attorney and see his or her membership record on the California Bar's website at **www.calbar.ca.gov**. After checking licenses you should go to the BBB website at **www.bbb.org/sdoc** to see the company's record with it.

After all this checking you should ask whether the advance fee covers just advice, i.e., a consultation, or advice and services. And if the latter, ask whether the solicitor is licensed to provide them and what services will be provided. Also ask what additional services might be involved and what they would cost.

Predatory Insurance Sales Practices

These practices involve insurance agents holding informational meetings or seminars about finances, living trusts as a way to avoid probate, or insurance investments that guarantee you will not outlive your retirement savings. These sessions are often held in senior centers, religious institutions, and restaurants. Attendees are required to sign in and give the agent their names, addresses, and phone numbers. Sometime after the session the agent, who may claim to be a "specialist" or "advisor," will contact the attendees to set up a meeting in their homes. It is in these one-on-one meetings that attendees can get pressured into buying an insurance product that is completely inappropriate for their needs. If you attend one of these information sessions you should not give any personal information to the agent. And you should talk to a trusted advisor before making any changes in your investments and insurance. Beware of limited-time offers and other tactics used to force you into a quick decision.

Although the vast majority of life insurance agents are honest, there are some who take advantage of persons whose trust they have gained, especially seniors, and take money from them to buy unnecessary insurance or annuities with promises of high returns. In some cases these financial predators convert the money to their own use.

To prevent this fraud you should first check the agent's license. It is required to be printed on all business cards, quotes, and advertisements. You can check it on the California Department of Insurance (CDI) website at **www.insurance.ca.gov**. Look under Agents & Brokers for the page entitled Checking License Status. You can check by name or license number. You should also check out the insurance company. In the CDI website look under Seniors on the page entitled Before You Buy Insurance and click on Check out the Insurance Company to verify that it is authorized to conduct business in California. You can also get this information by calling the CDI at **(800) 927-4357** between 8 a.m. and 5 p.m. Monday through Friday.

Before an agent can come to your home to discuss the sale of a life insurance or annuity policy, he or she must send you a written notice at least 24 hours before the meeting. The notice must include the reason for the meeting, and the names, license numbers, and phone numbers of all persons coming to your home. It must also state that: (1) others are invited to attend, e.g., family and friends, (2) you have the right to end the meeting at any time, (3) you have the right to contact the CDI for more information or to lodge a complaint, and (4) prior to purchase of a life or annuity policy you are entitled to a full disclosure of all surrender charges and related time frames in connection with the purchase. You must also be provided with all information relating to benefits and negative consequences regarding the replacement of an existing policy or annuity. Don't allow an agent to come to your home without sending you this notice. And if you do let him or her come, have a trusted advisor also attend. Never meet an agent alone. Remember that he or she is not a friend, but trying to appear as one. And never sign or pay for anything during the meeting.

If you are interested in any policy, get copies of everything involved, including promises and guarantees. Study them carefully and consult with your advisor before buying one. Then if you purchase a policy or annuity, you then have 30 days to review it. Then if you return it by the 30th day after you receive it, you are entitled to a full refund of your premium in a timely manner. If you believe you've been the target of insurance fraud, call the CDI consumer hotline at **(800) 927-4357** between 8 a.m. and 5 p.m. Monday through Friday.

Insurance agents also prey on military personnel before they deploy overseas. They take advantage of the emotional situation of leaving families at home and try to sell extremely overpriced or misrepresented life insurance policies. Military personnel desiring additional coverage should buy Service members Group Life Insurance (SGLI), which is a legitimate source for low premium policies. Service members have no need to buy private insurance.

Predatory Scams Targeted against Military Personnel

Here are some common scams and what to look for to avoid becoming a victim:

- In affinity scams a salesperson attempts to befriend and gain the trust of a person with similar religious beliefs, ethnic backgrounds, or military service in order to sell that person an overpriced, unnecessary, or nonexistent product. Don't trust anyone just because her or she has a military background, advertises in military newspapers or magazines, or has a business near your base. And don't trust a company just because it uses patriotic symbols or has a military-sounding name.
- In bait and switch scams an unethical salesperson may try to switch interest rates, terms and conditions, the model of the product, or other important details in a contract. Read the contract carefully before signing. Don't take the salesperson's word for anything in it.
- Be wary of pressure to act immediately. Take time to read the terms of the contract and discuss it with someone you trust. If something sounds too good to be true, it probably is.
- Predatory lending and mortgage foreclosure scams involve a wide variety of abusive practices and usually target borrowers with weak or blemished credit records. These include pressuring borrowers into taking out loans they cannot afford, urging borrowers to sign agreements without reading them, and charging excessive interest, prepayment penalties, balloon payments, hidden fees, etc. See the above sections on Bankruptcy Foreclosure Rescue, Predatory Insurance Sales Practices, and Pension Advance Loans for ways to avoid becoming a victim of them.

- One of the most common practices among predatory lenders is loan churning, where borrowers are forced into a relentless loan cycle in which they are constantly paying fees and interest, without noticeably reducing the principal amount owed on the loan. For example, some lenders have called veterans and offered to refinance their home loan so they could draw cash out and pay off other debts or credit card balances. The interest rate could be a half percentage point above the current market price. Then a few months later the lender would call back and offer to refinance at the lower market rate, earning another round of fees. In its November 2016 report entitled *A Snapshot of Servicemember Complaints: A Review of Issues Related to VA Mortgage Refinancing* at **https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/112016_cfpb_OSA_VA_refinance_snapshot.pdf**, the CFPB advised veterans as follows:
    - You don't have to respond to advertising. Although an ad may sound or look officially related to your veteran status or the VA, you don't have to refinance your home unless you decide it's in your best interest. Take a look at how long you will pay the new loan and whether the interest rate will change, not just at the monthly payment.
    - Be a savvy consumer. Look at everything an advertiser has to say about the product they're selling. Many times specific terms and conditions are hidden throughout the ad. Ask questions so you can be sure you know what you are signing up for.

In California the DBO administers a program called Troops Against Predatory Scams (TAP$). It educates California's troops on how to avoid becoming a victim of financial and investment fraud. TAP$ tells troops to confirm that salespeople and their company are properly licensed and registered, identifies possible "red flags" associated with the solicitations, directs troops to available resources, provides information on the current scams, etc. It also serves as the enforcement arm against financial fraud crimes by taking action against the predators targeting troops. Go to **www.dbo.ca.gov/Consumers/consumer_services.asp** to file a complaint against a licensee. Call **(866) 275-2677** if you need assistance with the complaint form or have any questions, concerns, or information about financial scams. TAP$ publications about investment fraud, predatory lending, and how to avoid being scammed can be downloaded at **www.dbo.ca.gov/Consumers/Education_Outreach/TAPS/Default.asp**.

TAP$ was established in 2005 under a grant from the Investor Protection Trust (IPT). The IPT is a nonprofit organization devoted to investor education. Since 1993 the IPT has worked with the States to provide the independent, objective investor education needed by all Americans to make informed investment decisions. More information about the IPT is available on its website at **www.investorprotection.org**. One of its publications is entitled *Financial Field Manual: The Personal Finance Guide for Military Families*. It can be downloaded from the IPT website at **www.investorprotection.org/downloads/IPT_Financial_Field_Manual_2012.pdf**. It also funded a booklet entitled *Protect You and Your Family from Fraud* that provides valuable information on investment and financial fraud, predatory sales practices, and scams directed at members of the military. It also includes information on privacy protection and managing financial difficulties, and a detailed resource guide. The booklet is online at **www.dbo.ca.gov/Consumers/TAPS/ Pubs/Taps_Booklet.pdf**. Although it was last revised in May 2009, it is still useful.

Prepaid Rental Listing Service

People who don't have the time or energy to look for a rental home or apartment often pay a Prepaid Rental Listing Service (PRLS) a fee to do a search for them and give them a list of rentals that meet their specifications. This sounds simple but scams are common. Not all PRLS businesses are licensed or honest. The dishonest ones may do the following:

- Engage in false advertising or representations concerning the services that will be provided
- List rentals that are not available as advertised
- List properties that are not for rent or do not exist
- List properties that do not meet your specifications
- Accept only cash
- Guarantee you will get a rental in your price range and location

- Provide a list of rentals that is handwritten, not computer-generated
- Does not provide property management or owner contact information for scheduling an appointment to visit the property. Says you should contact them instead.
- Give only first names
- Fail to provide refunds

The law covering PRLS is in the California BPC Secs. 10167 to 10167.17. Before paying a PRLS business a fee, make sure it is licensed by the CalBRE. You can do this on its website at **www2.dre.ca.gov/PublicASP/pplinfo.asp**. The business can be licensed as a PRLS or as a real estate broker. Don't deal with any unlicensed business. You should also do some research on any business you are considering using. Ask people you trust for recommendations. Check them out with the BBB. And go online and see what people are saying about them.

Before a licensee accepts a fee for a rental listing it must provide you with a written contract approved by the CalBRE that includes the following per California BPC Sec. 10167.9:

- The name and license number of the licensee and the address and telephone number of the principal office location of the licensee and the location, or branch office or a real estate broker providing the listing
- Acknowledgement of receipt of the fee, including the amount
- A description of the services to be performed
- Specification of the rental property you want found, including type of structure, location, furnished or unfurnished, number of bedroom, maximum acceptable monthly rental, etc.
- The contract expiration date, which shall not be later than 90 days from the date of execution of the contract.
- A clause setting forth the right to a full or partial refund of the fee paid as provided in Sec. 10167.10.
- The signature and printed full name of the licensee or of the designated agent, real estate salesperson, or employee acting on behalf of the licensee.
- A clause in bold type letters outlining the small claims court remedy available to the prospective tenant.

Prior to the acceptance of a fee, and in addition to the contract required pursuant to Sec. 10167.9, a licensee shall provide the prospective tenant with the following written notice, in a type size of at least 12-point type per Sec. 10167.95:

YOU MAY BE ENTITLED TO A REFUND IF YOU DO NOT RECEIVE THE SERVICES YOU HAVE BEEN PROMISED. COMPLETE TERMS AND CONDITIONS GOVERNING THE REFUND TO WHICH YOU MAY BE ENTITLED ARE CONTAINED IN YOUR CONTRACT. THE FOLLOWING IS A SIMLIFIED SUMMARY OF SOME OF THE RIGHTS DESCRIBED IN YOUR CONTRACT:

- You are entitled to a full refund from _____ if it does not provide you with at least three available rental properties meeting your specifications within five days after you pay the fee.
- You are entitled to a refund of your fee minus a service charge not to exceed $_____ if you do not obtain a rental through the services of _____ during the term of your contract.
- If _____ fails to refund your money as required by your contract, you may sue _____ in a small claims court. The court may award you the refund plus additional charges up to $1,000.

Additional information can be obtained from the following sources:

- CalBRE information at **www.calbre.ca.gov/Licensees/PRLS.html**
- CalBRE consumer fraud alert and warning at **www.dre.ca.gov/files/pdf/ca/2012/ConsumerAlert_PRLS.pdf**
- CalBRE warning regarding online rental schemes at **www.dre.ca.gov/files/pdf/ca/2013/ConsumerAlert_WarningRegardingOnlineRentalSchemes.pdf**

- Unlicensed businesses that have been issued orders to desist and refrain from engaging in further PRLS activities at **http://secure.dre.ca.gov/publicasp/prlsdnr.asp**.

Prize Notification and Lotteries

In this scam a person is notified by phone, e-mail, letter, or fax that he or she has won a prize and told to send the contest or lottery sponsor a signed release form and money to cover various expenses before the prize can be awarded. You lose not only the money but may provide the scammer with information for use in stealing your identity and committing various other financial crimes. Never respond to such a notice. Real prize winners don't have to pay a fee or taxes up front. If the notice came by mail, report the scam to U.S. Postal Inspection Service at **(877) 876-2455**.

In the case of lotteries, it is a federal crime to participate in a foreign lottery by mail, i.e., to send solicitations or payments for tickets. Most all foreign lottery solicitations sent by mail to U.S. addresses come from scam artists. Discard any you might receive. And don't provide any personal information. You can't win no matter what they say. Lotteries in the U.S. are illegal except when conducted by states and certain exempt charitable organizations.

In a variant of this scam the victim is approached by someone who says he or she has won the lottery and needs money to collect the winnings. The victim is told the money is just a loan and that it will be returned with a share of the winnings. This scam involves a ploy known as a "pigeon drop" in which the mark or "pigeon" is persuaded to give up a sum of money in order to get a larger sum in return. In reality, the scammers make off with the money and the mark is left with nothing. Walk away from anyone who offers you this kind of deal.

Property Tax Relief

Some companies have been offering to help homeowners reduce their property taxes for an up-front fee and not performing any reassessment or reassessment-appeal services. Their mailers featured official-looking logos and warned homeowners that their files would by ineligible for tax reassessments if they did not respond by a certain date. Homeowners should be wary of such solicitations and consider filing for property tax relief themselves. There is no cost for this. The procedure is explained on the website of the County Assessor/Recorder/County Clerk at **http://arcc.co.san-diego.ca.us**. Click on Reassessment/Ownership under Assessor Services, then on Proposition 13, and then on Application for Review of Assessment in the answer to the question: Can the assessed value of my property be decreased? You will get a page entitled "Property Tax Relief" and an Application for Review of Assessment. For additional information you can call the County Tax Assessor at **(858) 505-6262**.

Psychics

This scam can happen online, by phone, through the mail, and in person. Psychics have the skill to read your voice or your body language, find your vulnerabilities, and then play off your fears. And for a price they can cast a spell to stop bad luck, cure an illness, make someone love you, get you a good job, fix your negative aura, etc. The price will be in cash or a wire money transfer that doesn't leave a trail.

Do the following if you think you might be a victim of this scam:

- Stop all communications with the person.
- Don't give them any cash or wire them any money.
- If you live in San Diego, report your loss to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Otherwise report it to your local law enforcement agency.
- If you've lost money online, contact the FBI's IC3 at **www.ic3.gov**.

Rental Housing

Online ads make finding rental property very convenient for renters. But they also make scamming of unsuspecting or trusting renters easier. For example, in a Craigslist ad for a bargain vacation apartment rental in New York City the renter was told he had to act fast and wire the money or he'd lose out on this good deal. All three elements of a typical scam were present in this case: (1) act fast or lose the deal, (2) wire the money, and (3) a price that was too good to be true. Scammers use Craigslist, Zillow, Trulia, HotPads and other websites to advertise local rentals. Here are some things they might do:

- Duplicate or hijack an actual listing of property for rent, but with a lower price and a different contact number.
- Create a fake listing for a rental property.
- Offer for rent a real but unavailable property.
- Attempt to rent a property that is in foreclosure and will soon be sold, a property that has been foreclosed, or a property that is in pre-closure.
- Ask for cash upfront without showing the property or ask you to fill out a rental application with your SSN and other personal information.
- Say the supposed owner or rental agent is not available to show you the property, and pressures you to complete the transaction by e-mail as soon as possible.

Here are some tips for avoiding scams involving out-of-state rentals:

- Do an online search of the property address. It may reveal past scams there.
- Look at the address in an online aerial or street view to make sure the property exists.
- Walk away from any deal is which you are being pressured to make a fast decision.
- Don't rely solely on e-mail correspondence. Ask for a phone number and call it. Be wary of numbers with foreign or distant area codes.
- Be wary of e-mails in poor English.
- Never pay in advance with a debit card, wire transfer, or cash. A credit card is safer option.
- Check the rents of comparable property in the area and be suspicious if the rent is considerably lower.
- Don't give out any personal information such as SSN or bank account numbers in a rental application until you have verified that the rental is legitimate.
- Try to arrange vacation rentals through a real estate agency at your destination. The agency will handle payments, keys, etc. and may be able to help you resolve any problems that might arise during your stay.

For California properties:

- Verify the license of the rental agent. This can be done online at **www2.dre.ca.gov/PublicASP/pplinfo.asp** or by calling **(877) 373-4542**. Also ask to see an ID because the scammer might be using the name and license number of a legitimate licensee.
- Check the owner of the property with the county recorder. Confirm that the property is not in foreclosure or pre-foreclosure.
- Tour the property in person. Never rent property unseen.
- Insist on meeting the property owner or manger in person.
- Find out what comparable properties rent for.
- Never pay any money until you have received and reviewed all the rental documents.

See the section on Landlord Impersonation for things to do in dealing with scams involving rentals of vacant and foreclosed homes.

Reverse Mortgages

Reverse mortgages once had a bad reputation because scammers offered them to older homeowners as investment opportunities, foreclosure rescue, or refinancing assistance after recruiting them at local churches, investment seminars, direct mailings, and radio, TV, and other advertising. Changes to the Federal Housing Administration's Home Equity Conversion Mortgage (HECM) program in recent years have made them safer and less expensive. But seniors still need to be very careful in considering them. Here are some things they should do and not do.

- First, determine whether a reverse mortgage is right for you. The brochure entitled *Reverse Mortgages: Is One Right for You?* published by the CalBRE in the Department of Consumer Affairs should help. It's online at **www.calbre.ca.gov/files/pdf/re52.pdf**. It contains the potential advantages and drawbacks of a reverse mortgage, and the important questions to ask and things to do before making a decision. These include the following:
  - Does my home qualify for a reverse mortgage?
  - How much money do I need?
  - Decide how long you expect to stay in the home.
  - Is there a way to meet my needs that does not involve a reverse mortgage? Another kind of loan may be less costly.
  - Shop around and compare offerings. Not all reverse mortgages are the same. Their terms can vary substantially.
  - How much will it cost me in origination fees, closing costs, interest, monthly, or periodic fees?
  - Will a reverse mortgage make my partner or me ineligible for any "needs-based" public assistance benefits now or in the future?
  - Consult with a HUD-approved HECM counselor before you apply. A counselor can help you decide whether a reverse mortgage or some other alternative is best for you. None are listed in San Diego, however Credit.Org located in Riverside can provide counseling over the phone. Its number is **(800) 947-3752**.
  - If I die and my partner is still living in my home, will he or she have to leave or pay off the reverse mortgage?
  - Will the reverse mortgage become due and payable if I require long-term care and move to an assisted-living facility, or to a nursing or convalescent home?
- Don't respond to unsolicited ads for reverse mortgages or proposals for investing the proceeds from these mortgages.
- Make sure that any private professional fiduciary who handles your assets has a valid license from the California Department of Consumer Affairs PFB.
- Don't sign anything that you don't fully understand.
- Make sure your lender follows all the requirements of California Assembly Bill 329, the Reverse Mortgage Elder Protection Act of 2009. Except as specified, this Bill prohibits lenders from associating with any party that is associated with any other financial or insurance activity, and from referring the borrower to anyone for the purchase of an annuity or other financial or insurance product prior to the closing of the mortgage or the expiration of the right of the borrower to rescind the mortgage agreement. It also requires the lender to provide the borrower with a list of at least 10 counseling agencies in California approved by HUD, and a checklist of issues the borrower should discuss with a counselor. One issue is whether the prospective borrower's financial needs would be better met by other options like a less costly home equity line of credit. The checklist must be signed by the counselor and provided to the lender before the loan is approved. The lender is also required to inform the borrower that senior advocacy groups advise that you not use the proceeds of the mortgage to purchase an annuity or related financial products without discussing the financial implications with your counselor and family. These advocates have long cautioned that reverse mortgages should be a last resort because of their higher fees.

More recently in 2015 the CFPB warned consumers about being misled by reverse mortgage advertising. It said that reverse mortgage ads don't always tell the whole story so consumers should consider the following facts when they see ads.

- A reverse mortgage is a home loan, not a government benefit. They have fees and compounding interest that must be repaid, just like other home loans. With most reverse mortgages, federal insurance guarantees that borrowers will receive their loan funds if their lender has financial difficulty or if their loan balance exceeds the value of their home. However, borrowers pay for this insurance and it's not a government benefit.
- You can lose your home with a reverse mortgage. When a reverse mortgage ad says you'll retain ownership of your home, or that you can live there as long as you want to, don't take these messages at face value. They are true only if you continue to meet all requirements of the reverse mortgage. If you fall behind on your property taxes or homeowners insurance, are absent from your home for longer than six months, or fail to satisfy other requirements, you can trigger a loan default. If you don't take care of the default in time, the lender can foreclose on your home. Sometimes these requirements are listed in fine print, but not always. If you have a question about reverse mortgage requirements, contact a **HUD-approved housing counselor** near you.
- Without a good plan, you could outlive your loan money. After seeing a reverse mortgage ad, you might think that a reverse mortgage guarantees your financial security no matter how long you live. Americans are living longer today than they were just a generation ago. Make sure you have a financial plan in place that accounts for a long life. That way if you need to tap your home equity, you won't do it too early and risk running out of retirement resources later in life.

To obtain more information about reverse mortgages or to submit a complaint, call the CFPB at **(855) 411-2372** or visit its website at **www.consumerfinance.gov/askcfpb/**.

Short Sales of Homes

A short sale is an alternative to a foreclosure, which is a more time-consuming and costly process for the lender and the homeowner. In it the lender allows the homeowner to sell the property for less than what is owed on the existing mortgage and agrees to forgive some or all of the debt. The scam occurs when the agent or short-sale negotiator, who was hired by the homeowner, receives several bids but submits only the lowest. Unaware of higher bids, the homeowner and the lender accept that bid. This has the following effects. The lender loses the difference between the lowest and highest bid. The homeowner will have a greater tax liability if the debt cancellation, i.e., the difference between the debt and the sales price, is not covered by the Mortgage Forgiveness Debt Relief Act (MFDRA) of 2007. And the crooked agent or short-sale negotiator, who is also working with the lowest bidder, sells the property to the highest bidder and makes a sale profit in additional to his commission.

Because of the possibilities of fraud, tax liabilities (homeowners should note the MFDRA of 2007 expires at the end of 2013), and suits by the lenders to recover the forgiven debt, before you decide to sell through a short sale you should get: (1) a licensed and qualified real estate agent to represent you, (2) the advice of an accountant, and (3) the advice of an attorney. And then you need to look out for the following:

- Any short-sale negotiator must be a licensed real estate broker or a licensed real estate salesperson working under the supervision of a broker.
- Real estate licensees wishing to collect an advance fee must first submit an advance fee contract to the CalBRE and receive a no-objection letter for that contract. Then any advance fees paid must be placed in a trust account and handled as client trust funds.
- All payments must be fully disclosed and made a part of the escrow documents. Any fees paid outside of escrow are illegal.

- The buyer is a fictitious person or entity, or the buyer is purchasing the property under a power-of-attorney or limited liability company. This may indicate fraud.
- An unlicensed negotiator is handling the sale. This is illegal.

Staged Crashes

These are on the rise in many areas. According to the Auto Club of Southern California's Automotive Research Center (ARC) there were nearly 4,000 suspected fraudulent insurance claims in Los Angeles County in 2012 and 4,700 in 2014. Criminals pretend to be injured in staged crashes and bring large claims against the victim's insurance company. A common crash is called the" swoop and squat." In it a car suddenly cuts in front of you and stops abruptly so you can't avoid crashing into it from behind. In some cases an accomplice pulls alongside you to prevent you from swerving out of your lane to avoid the crash. For more information on staged crashes and videos on how they are set up go to the National Insurance Crime Bureau (NICB) website at **www.nicb.org** and check out the latest videos on insurance fraud and crime under Video/Audio Clips.

To reduce the risk of becoming a victim of a staged crash you should do the following:

- Never tailgate. In a typical staged-accident the perpetrators try to get you to rear-end them because it's a no-brainer for liability. If you hit a car from behind, you're likely to be at fault. So allow plenty of space between you and the car in front of you so you can stop if the vehicle in front of you stops.
- Pay attention. Look beyond the car in front of you for changed traffic conditions that might cause it to slow or stop. Don't wait for the vehicle in front of you to slow down before you apply your brakes. You're an easier target if you're not aware of traffic conditions.
- Look over your shoulder for better visibility when backing out of a parking space or driveway. Don't rely on your mirrors. And back out slowly.
- Drive defensively and be aware of your surroundings. Be extra cautious on freeway ramps, at stop signs, in parking lots, when merging into traffic, and making turns.

If you are ever involved in a crash, you should follow these tips from the Auto Club's ARC.

- Call **911** if anyone is injured.
- For each vehicle involved, get the name, address, phone number, driver license number, and auto insurance information for their drivers. Also get the names, addresses, and phone numbers of their passengers.
- Get the names, addresses, and phone numbers of anyone who witnessed the crash. Also get a written statement of where they were and what they saw. Or get a video of their statements.
- Take detailed photos of the crash scene, the damage to each vehicle involved, and people injured. The scammer might take his or her car to a body shop that's in on it scam, where the damage would be inflated for a higher claim. Without a photo it's hard to prove actual damage.
- Beware of tow trucks that arrive at the scene before anyone called for help. And don't let them take your vehicle, especially if they won't quote a charge. They may be planning to hold your vehicle until you pay an outrageous charge.
- Beware of strangers who appear on the scene and try to persuade you to take your vehicle to a certain body shop, hire a certain lawyer, or see a particular doctor. Or they may be working with the people who staged the crash to tell a story that is favorable to them.
- If you think you've been the victim of a staged crash, contact the local police and ask them to come to the scene. Get the names and badge numbers of the officers who arrive and ask for a copy of their report for your insurance company. Also report the staged crash to the NICB so the details can be added to its fraud data base.

Surprise Gift

In this scam you get a call from someone who says it's from a "delivery company" that has a gift for you and wants to know when you'll be home so you can sign for it. If you provide a time a uniformed delivery person will show up with the gift, which is a beautiful basket of flowers and a bottle of wine, and ask you pay a delivery charge of a few dollars by credit or debit card so there would be a record of the transaction. If you agree to do this the delivery person will swipe your card on a small, mobile card reader and print out a receipt for you to sign and another for you to keep. When asked about the sender, the delivery person says he didn't know who it is but there should be a card in the flowers.

The "delivery company" now has enough information to create a false card in your name. It will also have your PIN if you used a debit card. Then it can use the card at stores and ATM machines until you find out what is happening and notify the card issuer and close the accounts that were being drawn down. Here are some things you can do to avoid becoming a victim of this scam.

- Be wary of accepting any gifts of packages that you neither expected nor ordered, especially if you have to pay a delivery charge by credit or debit card.
- Never accept anything if you don't know who the sender it.
- Use a credit card instead of a debit card whenever possible. If your debit card information, including your PIN, is stolen your account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills.

Sweepstakes

These are advertising or promotional devices by which items of value (prizes) are awarded by chance to participating consumers, with no purchase or entry fee required to win. They differ from lotteries where participants pay for a chance to win a prize.

The Deceptive Mail Prevention and Enforcement Act of 1999 grants increased powers to the U.S. Postal Service to better protect consumers from those who use deceptive mailings in promoting sweepstakes. It prohibits the following in offers:

- Saying the recipient is a winner unless that person has actually won a prize
- The recipient must make a purchase to enter. If separate YES and NO response envelopes are used, NO responses receive equal treatment in the sweepstakes. YES responses just help the sponsor fill orders promptly.
- Payment for a previous purchase must be sent with an entry
- The recipient must make a purchase in order to receive future sweepstakes mailings
- Sending a fake check without a statement on it that it is non-negotiable and has no cash value
- Use of any seal, name, or term that implies a federal government connection, approval, or endorsement

For more information, see the U.S. Postal Service Publication 546 entitled *A Consumer's Guide to Sweepstakes and Lotteries*. It's online at **http://about.usps.com/publications/ pub546/welcome.htm**. If you think you've been victimized by a fraudulent offer you can contact the U.S. Postal Service Inspection Service at **(877) 876-2455** or file an online complaint for mail fraud at **https://postalinspectors.uspis.gov/contactUs/ filecomplaint.aspx**.

Sweetheart or Romance Scams and Online Dating

Sweetheart or romance scammers typically prey on older people who want to start dating again after a divorce or the death of a spouse. They troll the Internet to make a love connection that they can exploit in various ways. In short, they pretend to be in love and then asking for money. According to the FBI's IC3, which provides the public with a means of reporting Internet-facilitated crimes, sweetheart or romance

scams, also called confidence fraud, result in the highest amount of financial losses to victims when compared to other Internet crimes. In 2016 nearly 15,000 complaints of these scams were reported to IC3, versus 12,500 in 2015. The losses associated with those complaints exceeded $230 million. California is one of the states with the highest numbers of victims.

There are several reasons for the rise in these crimes. First, when someone uses a computer, it's possible to find out where the computer is but it's very hard to find out who's using it. And then it's difficult to prove the crime. These crimes are lucrative and easy to commit. And the scammer can remain anonymous and beyond the reach of authorities.

To avoid becoming a victim in these scams you should use great caution and common sense in dealing with someone you haven't met in person, especially if they say that this romance is destiny or fate and that we were meant to be together. And beware if a person says they cannot live without you but they need you to send money so they can visit you. Never send money to someone that you have not met in person, no matter how compelling or heart-wrenching their story may be. Don't let your "love" for your online suitor to allow you to be robbed blind. Beware of a person that does any of the following:

- Requests that you wire money to them for any number of reasons, e.g., to pay a hospital bill, buy an airplane ticket to come visit, start a business, etc.
- Requests that you cash a check or money order for them and send the cash back or to a third person. Asks you to forwarding a package. In reality, they are looking for help in laundering money by cashing phony checks and sending money overseas or shipping stolen goods.
- Makes pronouncements of love or close friendship early on.
- Claims that he or she is a U.S. citizen who is abroad, wealthy, and of high status.
- Claims to be a contractor and needs your help with a business deal.
- Makes excuses about not being able to speak by phone or meet in person.
- Asks for an e-mail address or instant messaging username to avoid communication via online dating sites' messaging services.
- Makes frequent spelling or grammar mistakes in writing and speaking.
- Asks for your street address for mailing a gift.

With online dating being more popular than ever, scammers have a golden opportunity to take advantage of unsuspecting men and women and make fast money through a variety of scams. In a typical scam the scammer will create a fake online dating profile complete with attractive photos and then reach out one-on-one via e-mail, chat, text, or phone to establish a relationship and thereby gain trust. Once trust is established they may ask for money for a plane ticket to visit or to help them with a tragic incident. For instance, the scammers may say that they have a life-threatening illness or they need money to pay rent. Other signs that your suitor is only interested in your money include professing instant love and pressing you to leave the dating website you met through and communicate using personal e-mail or instant messaging. You should communicate through the website's e-mail/messaging services as long as possible because they offer some privacy protection. Or consider creating a separate e-mail address solely for online dating. If you do share a personal e-mail address and later something goes wrong, you won't be receiving unwanted e-mails to your primary account.

In a news story entitled *Romance Scams: Online Imposters Break Hearts and Bank Accounts* dated Feb. 13, 2017 and published online by the FBI at **www.fbi.gov/news/stories/romance-scams**, it is suggested that you do the following before you develop a romantic relationship with someone you've "met" online.

- Research the person's photo and profile using online searches to see if the material has been used elsewhere.
- Go slow and ask lots of questions.
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or Facebook to go "offline."

- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
- Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you don't know personally.
- If you suspect an online relationship is a scam, stop all contact immediately. And if you are the victim of a scam, file a complaint with the FBI's IC3 at **www.ic3.gov**.

Here are some other tips for staying safe and avoiding scammers.

- Limit the amount of personal information you post online and use privacy settings to control who can see it.
- Stick to reputable dating websites to avoid scammers.
- If you choose to meet someone you've "met" online, pick a public place like a coffee shop, let others know where you are going beforehand, and be cautious of what personal information you disclose about yourself.
- Restrict your search to singles that are within driving distance of your community so if you find someone you'd like to meet, doing so will be feasible. Scammers often claim to be U.S. citizens who are working or traveling abroad. Be on high alert if someone claims to be away for an extended period.
- Don't share too much information about yourself online or when you are in the very early stages of a relationship. Potential dates don't need to know your last name, your place of employment, or other details about your daily life and routines. That information can be shared later, over time.
- Never send money to anyone you connect with online, even if you believe you have a legitimate "virtual relationship." Cease communication immediately with anyone who asks for money regardless of the situation or "emergency." You will never see the money again, despite promises to pay you back promptly.
- It is better not to engage in video conferencing before you have met someone in person.
- Never engage in sexual or explicit behavior using a web camera. Scammers are known to save these images and threaten to send them to your relatives and friends unless you send money. Or they post intimate conversations along with your name and phone number on a website and say you need to pay to have it removed.
- Talk about your online dating experiences with trusted relatives and friends. They may be able to spot warning signs that you've missed.
- Always remember that you don't really know who you are dealing with until you have met and gotten to know them.

Tax Debt Relief

Beware of attorneys, accountants, and others who offer to make your IRS tax debt vanish for an upfront fee. Most of the time it's your money that will vanish while IRS interest and penalties continue to grow. You can contact in the IRS several ways to get information about your account. If you have a mobile phone you can find out how much you owe by using the tool in the IRS website at **www.irs.gov/payments/finding-out-how-much-you-owe?_ga=1.114060996.276758516.1455138335**. To register for this service, you need to provide the following: your SSN, date of birth, filing status, and mailing address from latest tax return; access to your e-mail account; and your personal account number from a credit card, mortgage, home equity loan, home equity line of credit or car loan; and a mobile phone with your name on the account. Then you can find out your payoff amount and the balance for each tax year for which you owe. If you don't have a mobile phone you can call **(800) 829-1040** for assistance. But before you do, you should go to **www.irs.gov/help-resources/telephone-assistance** for links to information on payments and penalties and then have the flowing information handy: your SSN, birth date, and filing status; a copy of the tax return you are calling about; and letters of notices from the IRS regarding this return.

If you owe back taxes or have a tax debt you cannot pay, contact the IRS as soon as possible. There are several programs for taxpayers who cannot afford to pay their debts. The options are described on the IRS website at **https://www.irs.gov/taxtopics/tc202.html**. They include the following:

- Short-term Full Payment Agreement. If you owe more tax than you can pay, you may qualify for more time, up to 120 days, to pay in full. You do not have to pay a user fee for this but the IRS will charge interest and applicable penalties until you pay in full. You can apply for this online at **www.irs.gov/individuals/online-payment-agreement-application**. You can call the IRS at **(800) 829-1040** for more information. And if you have questions about a bill from the IRS, you can call the phone number listed on it.
- Installment Agreement. If you are unable to pay your balance in full immediately, you may qualify for a monthly installment agreement. You can apply for this online at **www.irs.gov/individuals/online-payment-agreement-application** or complete IRS Form 9465 entitled *Installment Agreement Request* at **www.irs.gov/uac/about-form-9465** and mail it to the IRS. An installment agreement allows you to make a series of monthly payments over time by payroll deduction from your employer or payments by the EFTPS, credit card via phone or Internet, or check or money order. Each of these options has a different one-time user fee.
- Offer in Compromise (OIC). If you cannot pay in full and an installment agreement will not work, you may want to propose an OIC, which is an agreement between you and the IRS that resolves your tax liability by payment of an agreed upon reduced amount. To confirm eligibility, use the Offer in Compromise Pre-Qualifier tool at **http://irs.treasury.gov/oic_pre_qualifier/**. The questionnaire format assists in gathering the information needed and provides instant feedback as to your eligibility based on the information you provided. The tool will also assist you in determining a preliminary offer amount for consideration of an acceptable offer. For additional information on OICs, refer to **www.irs.gov/individuals/offer-in-compromise-1**.
- Temporarily Delay Collection. If you cannot pay any of the amount due because payment would prevent you from meeting your basic living expenses, you can request that the IRS delay collection until you are able to pay. If the IRS determines that you cannot pay any of your tax debt because of financial hardship, the IRS may temporarily delay collection by reporting your account as currently not collectible until your financial condition improves. Being currently not collectible does not mean the debt goes away. It means the IRS has determined you cannot afford to pay the debt at this time. Penalties and interest will continue to accrue until you have paid off the debt in full. Prior to approving your request to delay collection the IRS may ask you to complete a Collection Information Statement using Form 433-F, -A, or -B and provide proof of your financial status, which may include information about your assets and your monthly income and expenses. More information on the collection process can be found at **www.irs.gov/taxtopics/tc201.html**.

You can also get help in tax debt relief from the Taxpayer Advocate Service (TAS), an independent office within the IRS. It offers free, independent, and confidential assistance to taxpayers who are unable to resolve their tax problems through normal channels or are experiencing financial hardships. The nearest TAS office is in Laguna Niguel. You can call **(949) 389-4804** for an appointment.

Tax Return and Refund Fraud

One way this scam can occur is when an identity thief submits a federal tax return with a stolen SSN and phony wage and tax withholding figures. Then he or she claims a refund by a check to be mailed to a certain address, a direct deposit into a bank account he or she controls, or a deposit onto a prepaid debit card. Anyone with a SSN could become a victim. However, these scammers seem to focus more on people who don't normally file tax returns, i.e., the elderly, low-income families, students, a child, a dead person, patients at long-term health care facilities, non-English speakers, and even the homeless.

From January through April 2016 the IRS stopped $1.1 billion in fraudulent refunds claimed by identity thieves on more than 171,000 tax returns compared to $754 million in fraudulent refunds claimed on 141,000 returns

for the same period in 2015. Better data from returns and information about schemes meant better internal processing filters to identify identity fraudulent tax returns. The IRS also suspended for further review 36,000 suspicious returns and $148 million in claimed refunds in 2016 compared to 15,000 suspicious returns claiming $98 million in refunds in 2015.

If you believe your SSN has been compromised, contact the IRS Identity Protection Specialized Unit (IPSU) at **(800) 908-4490**. The IPSU will suggest that you file an IRS Form 14039, Identity Theft Affidavit. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. It will authorize the IRS to put a marker on your account that will help it protect you from identity theft and resolve future identity theft issues. The IRS will also give you a 6-digit Identity Protection PIN (IP PIN) to use on your Forms 1040, 1040A, 1040EZ or 1040PR/SS. The IP PIN will change every year. Any returns with an incorrect IP PIN will be rejected.

If an identity thief has used your SSN to file a tax return in an attempt to get a fraudulent tax refund early in the filing season and you file your own return later, you will receive a notice or letter from the IRS that states one of the following: (1) More than one tax return for you has been filed, (2) You have to return the money paid out in your name to the identity thief, or (3) IRS records indicate you received wages from an employer not names on your return. In this case you will need to respond immediately and submit the Form 14039. If you are experiencing economic harm or the problem is not being resolved through normal channels you can get help from the TAS by calling **(877) 777-4778**. More information on the TAS is available at **www.irs.gov/advocate**.

Here's what the IRS Summertime Tax Tip 2017-16 dated August 7, 2017 says you should do if you can't e-file because someone already filed using your SSN.

- File a tax return by paper and pay any taxes owed.
- Fill out an IRS Form 14039 and attach it to your paper tax return, and attach a police report describing the identity theft if one is available.
- File a report with the FTC using the Complaint Assistant at **www.ftccomplaintassistant.gov/ #crnt&panel1-1**.
- Go to **https://search.ssa.gov/search?utf8=%E2%9C%93&affiliate=ssa&query= identity+theft&commit=Search** on the SSA website for links to material on what to do if your SSN is stolen and used fraudulently.
- Inform your financial institutions about the identity theft.
- Request that the Consumer Credit Reporting Bureaus (CCRBs) place an extended fraud alert on your credit reports. They are free and good for seven years. They permit some creditors to get your report as long as they take steps to verify your identity, which may include contacting you in person. Like an initial fraud alert, an extended alert may prevent someone from opening a new account in your name but it will not prevent misuse of your existing accounts. The bureau you contact is required to inform the other two. Equifax has an online request form at **www.alerts.equifax.com/ AutoFraud_Online/pdf/ Fraud_Alert_7.pdf**. Experian's is at **www.experian.com/consumer/cac/PrepopulatedForm.do? PrePopulatedForm.No=1017&type=victim**. Information on placing a request with TransUnion can be obtained by calling **(800) 680-7289**. You will have to provide a copy of a police report, proof of your identity, and other information with these requests.
- An alternative to an extended fraud alert is a security or credit freeze. A freeze generally stops all access to your credit files, but like a fraud alert, it may not stop misuse of your existing accounts or other types of identity theft. You can place freezes on your credit reports by contacting each CCRB: Equifax at **(800) 349-9960**, Experian at **(888) 397-3742**, and TransUnion at **(888) 909-8872**. Or you can request a freeze online at these websites: **www.freeze.equifax.com**, **www.experian.com/ freeze/center.html**, and **www.transunion.com/credit-freeze/place-credit-freeze**. You'll need to supply your name, address, date of birth, SSN, and other personal information. Fees vary based on your age and where you live, but commonly range up to $10. After receiving your freeze request by phone, each CCRB will send you a

confirmation letter containing a unique PIN or password to use if you choose to lift the freeze. If you request a freeze online, you can download your PIN.
- Complete and submit Form 3552 if you are an actual or potential victim of identity theft and would like the California Franchise Tax Board (FTB) to update your account status to identify questionable activity. The form is on the FTB website at **www.ftb.ca.gov/forms/misc/3552.pdf**.

If you have not become a victim or had your SSN compromised, you can get a PIN to prevent the misuse of your SSN on fraudulent tax returns. The steps for getting an IP PIN are in **www.irs.gov/Individuals/Get-An_Identity-Protection-PIN**. Those for getting an Electronic Filing PIN are in **www.irs.gov/Individuals/Electronic-Filing-PIN-Request**.

Other things you can do to prevent this scam in addition to those for protecting your SSN and other personal information are in the SDPD paper entitled *Identity Theft Prevention and Victim Responses* at **www.sandiego.gov/sites/default/files/identitytheftpreventionandvictimresources.pdf**

- Go to **www.irs.gov/Individuals/Identity-Protection** for links to information on identity theft prevention, detection, and victim assistance.
- Order a transcript of your IRS account at **www.irs.gov/Individuals/Get-Transcript** to see what tax payments and refunds the IRS has on record for you.
- File your returns early to limit fraud opportunities in the current filing period.
- Mail returns from a post office, not from your home.
- Use a secure Internet connection when filing electronically. Do not use unsecure, publicly available Wi-Fi hotspots.
- Monitor your bank accounts at least once a week and notify your bank immediately if you see something you didn't authorize.
- Go to **www.irs.gov/uac/Tax-Scams-Consumer-Alerts** for details of ongoing and recent tax scams and tips on how to avoid them.

Another way this scam can occur is when taxpayer hires a dishonest tax preparer who touts inflated tax refunds. See the above section entitled *Dishonest Tax Return Preparers* for ways to avoid dishonest tax preparers and hire an honest one. If you participate in this scam, you may receive a significant penalty, imprisonment, or both. Simply filing a false tax return may result in a $5,000 penalty.

If you want to know the status of your claimed refund, you can go to **www.irs.gov/refunds** and use the "Where's My Refund?" tool. It can be checked 24 hours after the IRS has received an e-filed return, or four weeks after receipt of a mailed paper return. Users must have their SSN, filing status, and the exact amount of the refund to find out its status, which will be displayed in three stages: (1) return received, (2) refund approved and (3) refund sent.

Tech Support for Computers

Scammers, often pretending to be from a well-known company like Microsoft or Apple, may call you at home, place pop-up messages on your computer, or offer free computer security scans to alert you to non-existent viruses or other malware on your computer and then offer to remove them. If you accept their offer they might do the following.

- Ask you to give them remote access to your computer so, while pretending to fix the problem, they can change settings to make it vulnerable to attack, install malware to enable them to steal sensitive personal, financial, and computer information, etc.
- Try to sell you software that's worthless, or that you could get elsewhere for free
- Try to enroll you in a computer maintenance or warranty program that's worthless
- Ask for credit card information so they can bill you for their services in fixing the a non-existent problem

To avoid these problems, here are some things to do if you get an unexpected offer of tech support to fix a problem with your computer.

- Hang up if you get an unexpected call. It's a scam. And don't rely on Caller ID to identify the caller. Scammers can spoof Caller ID to make it show a legitimate company or a local number.
- Ignore a pop-up message. Don't call any number that appears on it. Call your computer security company directly if you're concerned about your computer. Use the contact number on its website or any documentation from it. And don't click on any links.
- Be suspicious of any e-mail that asks for personal or financial information, says it's urgent, or contains a link to a website that does not match the organization sending the e-mail.
- Never give control of your computer to anyone who calls and offers to fix your computer, e.g., saying that your e-mail account has been hacked and you need to act immediately to keep it sending out fraudulent messages to everyone in your address book.
- Never share passwords or give control of your computer to anyone who contacts you unless you can confirm that the party is a legitimate representative of a company you already deal with. Change any passwords you did share.
- Don't pay for any services, which are usually for fixing a non-existent problem. If you paid for any bogus services with a credit card, call your credit card company and ask to cancel the charges. And check your credit-card statements for any charges you didn't make. Ask to cancel them too.
- Run a security scan on your computer. Delete anything that's identified as a problem.

If you're tempted by an offer of a free computer security scan, be prepared to be told that your computer has a whole host of problems and that you need to update your security software, which can be very expensive. Rather than rush into downloading new software, check that your existing security software is active and current, and includes at least anti-virus and anti-spyware software, and a firewall. You can buy stand-alone programs for each element or a security suite that includes these programs from a variety of sources, including commercial vendors and your Internet Service Provider (ISP). You should also call the Better Business Bureau (BBB) of San Diego, Orange, and Imperial Counties at **(858) 496-2131** to check on any computer repair companies that advertise on the Internet before you respond to any ads. Or visit its website at **www.bbb.org/sdoc** to see whether the company is accredited, check its rating, reason for the rating, the complaint history.

On April 8, 2014 Microsoft ended its support and updates for Windows XP. This means there will be no more security updates, non-security hot fixes, free or paid assisted support options, and online technical content updates for computers with the Windows XP operating system. You can get more details on the end of XP support at **www.microsoft.com/en-us/WindowsForBusiness/end-of-xp-support**. Users who continue to run XP after the end-of-support date become very attractive targets for malicious scammers. To avoid these risks Microsoft suggests that users upgrade their PCs with a modern operating system or if that is not possible, to buy a new PC. If you continue to use XP, in addition to the above measures for dealing with fake help desk scams, you should do the following.

- Switch to Google Chrome or Mozilla Firefox for web browsing. Both will work with XP and have the latest browser security features.
- Stick to trusted websites.
- Don't do online banking, shopping, or anything that involves personal or financial information.
- Remove software you don't need.

The best thing to do is disconnect your XP computer from the Internet and use it just for word processing, spreadsheets, or games that are already installed on it. And be careful about attaching USB storage drives as they might introduce malware.

Third-Party Telephone Bill Charges

This telemarketing scam involves the sale of some kind of service. The caller gets you to say "yes" to some question and then mails you information about the service. The mailing looks like junk mail and the caller hopes you will throw it away without reading it because it says that you have some period of time to cancel the service. When you fail to reply, a monthly service fee is added to your phone bill. If you dispute the fee the caller will produce an edited version of the phone conversation in which you agreed to receive information about the service and pay the monthly fees. To avoid these problems you should do the following:

- Hang up immediately on any unsolicited callers. Don't get involved in a conversation. And never say "yes" to any question.
- Open all mail, even if it looks like junk mail. There might be something you need to do to prevent being billed for some service you didn't request or don't need.
- Examine your phone bill for third-party charges. Don't pay any that you did not authorize and report them immediately to the phone company.

Timeshare Transactions

You need to be careful when you buy or sell a TimeShare (T/S). Scams exist in both of these transactions. Beware in buying a T/S if you are told any of the following:

- Your T/S is an investment that will increase in value.
- You can rent your T/S to make money.
- Your maintenance fees will not go up, but if they do, it will only be by a small amount.
- This special sales offer is only good today.
- The sales presentation will only last 90 minutes
- The company will buy your previous T/S for a great profit to you.
- You can go anywhere in the world whenever you want.
- You have a legal right to rescind or cancel the contract whenever you chose.

If you sign a contract to buy a T/S and later have regrets, beware of "attorneys" who offer to get you out of your contract. They will want an upfront fee and will probably do no more than send a letter to the T/S seller demanding that the contract be cancelled.

Most scams occur when you try to sell a T/S. These usually involve some sort of an upfront fee paid to a company who says it will help you sell your T/S. It may say it has a buyer already, it just sold one like yours and knows its market value, or it guarantees to sell yours. Then it asks you will pay an upfront fee for its work. It will also say your fee is refundable if your T/S doesn't sell. Once the fee is paid, the company disappears. You should never pay an upfront fee. And if you want to recover your upfront fee, beware of "attorneys" who offer to help for another upfront fee. In a variant of this scam the company offers to take your T/S off your hands for an upfront fee so you won't have to continue paying its maintenance fees. All it does is change the address where the maintenance bills are sent so you think there was a transfer of ownership. You are still responsible for those fees.

Another scam involves a company that says your T/S's worthless but offers to buy it for a small amount. The company also says that you will no longer have to make payments on the T/S, and that your loss is tax deductible. Then the company offers to sell you a worthless travel club membership for more than it's paying for your T/S. If you agree to buy it you end up paying the difference, giving up your T/S, which the company can sell for an additional profit, and not getting the promised tax benefit.

Then there's the scam in which a buyer gives you a cashier's check for more than the sales price and asks you to deposit it in your bank and wire back the difference. When the check is found to be counterfeit it will be

returned to your bank and the full amount deducted from your account. You can avoid this problem by not cashing the check in the first place, but if you do you should wait until it clears before withdrawing any of it. See the section above on fraudulent check for more about this kind of scam.

There are no surefire ways to detect scammers. Here are some things a scammer might say, do, or not do that will help you avoid becoming a victim.

- Requests upfront fees before any services have been performed.
- Requests that you pay only in cash or by wire transfer, money order, certified bank check, or cashier's check. Unlike payment by credit card, these forms of payment provide little if any recourse after you have paid the scammer.
- Is unwilling to meet you in person or give you a business phone number, address, or card. Uses a Post Office box for mail.
- Says you don't have to read or understand the documents you are asked to sign.
- Says you must act immediately, and should not talk to your family, attorney, accountant, or anyone else about the sale.
- Claims that the market for your T/S is very good at this time.
- Guarantees that your T/S will sell within a certain period of time, or you can get your money back.
- Requests personal financial information over the phone or the Internet.
- Says you can "walk away" from you timeshare by transferring it to some third party.

If you are considering reselling a T/S, you should:

- Check with the developer of your T/S to see if it offers a resale or buyback program, or has an affiliated broker that handles resales. If it does, it may be easier and safer to deal directly with it.
- Be wary and cautious when thinking about retaining the services of people and companies offering assistance in T/S resales.
- Never pay for services or assistance in advance of the performance of services.
- Make sure the person offering to list and resell your T/S is a licensed real estate broker or a licensed sales person working for a licensed broker. You can check license numbers and disciplinary actions on the CalBRE website at **www2.dre.ca.gov/PublicASP/pplinfo.asp**. Call the licensed broker to verify that the person you are dealing with actually works for it.
- Request a copy of the written contract that you and your agent will be required to sign along with a written disclosure of all fees and costs. Read all the fine print. Get help from an attorney if you don't understand anything.
- Check with the BBB to ensure that the company is reputable.

Don't be afraid to ask questions. Legitimate agents and companies should not mind answering them. Here are a few you might ask.

- May I see your license?
- How many T/S resales have you made? Ask for some specifics and check them out.
- Do you have a list of past T/S sellers? If so, get it and call some to ask if they were pleased with their resales.
- Do you have a list of business and banking references? If so, get it and call check them out.
- How long have you and your company been doing T/S resales?
- What are you actually going to do to market my T/S?

For more information on T/S resale fraud go to the Consumer Alerts page of the CalBRE website at **www.dre.ca.gov/Consumers/ConsumerAlerts.html** to see the March 2012 warning regarding timeshare resale fraud and the February 2013 warning regarding latest timeshare fraud scheme involving wire transfers. For general information on T/S sales go to the Timeshare Resales page on the American Resort Development Association-Resort Owners Coalition's website at **www.arda-roc.org/ roc/resource-library**.

Travel Reservations

This scam involves fake hotel and third-party reservation websites in which a scammer keeps your room deposit, credit card information, etc. and leaves you without a reservation. In fake hotel websites the scammers replicate real hotel websites using copyrighted images, trademarked logos, toll-free phone numbers, and similar URLs. When you arrive you may find no reservation, or if there is one, you may find your special requests have not been honored, the rate is higher than that advertised, and there are undisclosed fees. You may also have trouble canceling or modifying your reservation, cancelling disputed credit card charges, and getting credit for points in the hotel's reward program. To avoid these problems and because it can be hard to tell whether you're on a hotel's website, to make a reservation you should find the hotel's phone number yourself and call it to confirm that you're dealing with the actual hotel.

In fake third-party reservation websites the scammers usually have many different hotel options. If you want to make reservations with a third-party and avoid the problems cited above, you should use a well-known reputable company and be careful when entering its URL in your Internet browser. Otherwise, book directly with a hotel as suggested above.

Unclaimed Funds

There are several scams involving unclaimed funds. One usually starts with an e-mail telling you about all the unclaimed money in the country and offering to do a free search for you for only a share of the money found for you providing you call immediately on an **809**-area code number, which is in the Bahamas. What you're not told is that **809** calls are very expensive and the scammers get a share of the cost from the foreign telephone company, the search will be cursory, and you will be asked to provide personal information and pay a fee for a more complete search. Not only should you never dial an **809** number or give out personal information, but you can easily do the search yourself on the Internet. You can do it by state on the National Association of Unclaimed Property Administrator's website at **www.unclaimed.org**. If you click on California you will go to a page on the website of the State Controller's Office where you can do a search by individual owner, business/government, or property ID. You can go to this page directly at **www.sco.ca.gov/upd_msg.html** or you can call **(800) 992-4647** to make a claim, check the status of a claim, etc.

Another scam involves imposters who use your identity to obtain unclaimed funds in your name. And then there's the one in which people have received e-mails from individuals who claim to work for the State Controller. These e-mails instruct the recipient to contact a private attorney for assistance in recovering their lost and abandoned property, including that from a relative's estate. The State Controller warns that it does not send out unsolicited e-mails about unclaimed property, nor would it refer individuals to a private attorney. It is a violation of state law for individuals and companies to falsely identify themselves as representing a state official. If you receive similar solicitations, forward them to the Controller at **EOInquiry@sco.ca.gov** so its legal office can take appropriate action. The Controller strongly recommends that you not respond to these false solicitations, as the senders are seeking personal information and will charge fees for recovering property that you can obtain at no cost as suggested above.

Unlicensed Payday Lenders

Payday loans are high-interest, short-term loans designed to provide advances on paychecks. Many payday lenders are now operating online and not registering with the California DBO. Lenders who do register must comply with California laws, including truth-in-lending statutes. Unlicensed lenders may not even be in California. Furthermore, you may not be able to contact them if you run into trouble, you have no recourse if you are ripped off, and your private financial information may not be protected against identity theft. Before doing business with an online payday lender, make sure the lender is licensed with the California DBO. You can verify the license online at **http://search.dre.ca.gov/integrationaspcode/** or by calling **(866) 275-2677**.

Virtual Kidnapping

This is an extortion scam in which a caller pretends to have kidnapped a relative or friend and demands ransom. Scammers will often threaten extreme violence and convey personal information about the "kidnapped" person to make the call appear credible. They will demand you go to your bank, withdraw the money, and either meet them with it, or wire it to their bank. This scam depends on you panicking and believing that the scammers actually have the person.

Any call you receive like this is usually a scam, but to be sure look for the following:

- Call is from an outside area code or foreign country
- Call is not from the person's phone
- Caller goes to great length to keep you on the phone so you can't attempt to call or locate the person
- Ransom money is only accepted via wire transfer service

If you receive an extortion call, the FBI suggests you first request to speak to the person directly. Ask "How do I know my loved one is OK?" If they don't let you speak to the person, request the person call back from his or her cell phone. And while staying on the line with "kidnappers," attempt to call, text, or otherwise contact the person from another phone. Or say you will call back to the person's cell phone.

Weight-Loss Products

Products advertised with miracle ingredients, testimonials of permanent weight loss, or claims of quick and easy **www.ic3.gov www.ic3.gov www.ic3.gov** weight loss without dieting or exercising are scams. They're a waste of money and may also be harmful. For example, some contain more than a moderate daily dose of caffeine. Always consult your physician before using any weight-loss product. And buy supplements only from retailers and manufacturers you trust. Look for third-party seals of approval like those of the U. S. Pharmacopeial Convention (USP). You can get links to view USP

Verified products on its website at **USPVerified@USP.org** under Dietary Supplements and Verification Services. Or you can call USP at **(301) 816-8273** with questions about specific products.

Wiring Mortgage Closing Costs

Hackers have been breaking into some real estate agents' and home buyers' e-mail accounts to get information about upcoming transactions. After figuring out the closing dates, the hacker sends an e-mail to the buyer posing as the agent or settlement agent, i.e., title company, escrow officer, or attorney. The bogus e-mail says there has been a last-minute change to the wiring instructions and tells the buyer to wire or otherwise electronically transmit the closing costs to a different account, which happens to belong to the hacker. If the buyer takes the bait, its bank account could be cleared out in a matter of minutes. So if you're buying a home, here are so things you should do to avoid this scam.

- Discuss the closing process and money transfer protocols with your real estate or settlement agent in advance. Agree who will contact whom on settlement day to receive the wiring details, and who will manage the wiring process. In any case, don't use e-mail in financial transactions or for transmitting financial information. It's not secure. And if you give any financial information on the web, make sure the site is secure, i.e., its URL begins with **https**.
- If you get an e-mail with money-wiring instructions, contact your real estate or settlement agent, in person if possible, or else over the phone, to confirm the change before wiring any money. Don't use any phone numbers or links in the e-mail for this.
- Be cautious about opening attachments and downloading files from e-mails, regardless of who sent them. These files can contain malware that can weaken your computer's security.

- Never wire money based on the say-so of one party to the transaction made via e-mail. You simply don't know if their account is hacked. So from a self-preservation standpoint, it's best to assume it is. Always double or even triple check any instructions for wiring money at settlement.
- Before sending any wire transfer, ask your bank for help identifying any red flags in the wiring instructions. These include potential discrepancies between the account name and the name of the intended beneficiary, i.e., your real estate or settlement agent. Your bank may also be able to compare the receiving account number to account numbers identified in past consumer complaints as the destination of fraudulent transactions.
- Confirm receipt of the wire transfer by your real estate or settlement agent a few hours after the wire was transmitted. If you or another entity involved in the closing suspect a problem, report it to law enforcement and your bank as soon as possible to increase your likelihood of recovering the money.
- Contact your bank or the money transfer company immediately upon discovering that funds have been transferred to the wrong account. Ask the bank or money transfer company to attempt a wire recall.

This scam also has lessons for real estate agents. They should improve their e-mail security, and give their clients a written notice that they will never send wiring instructions by e-mail.