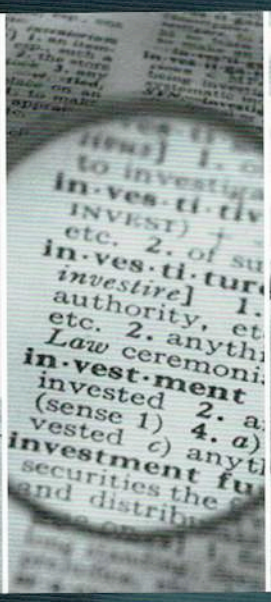
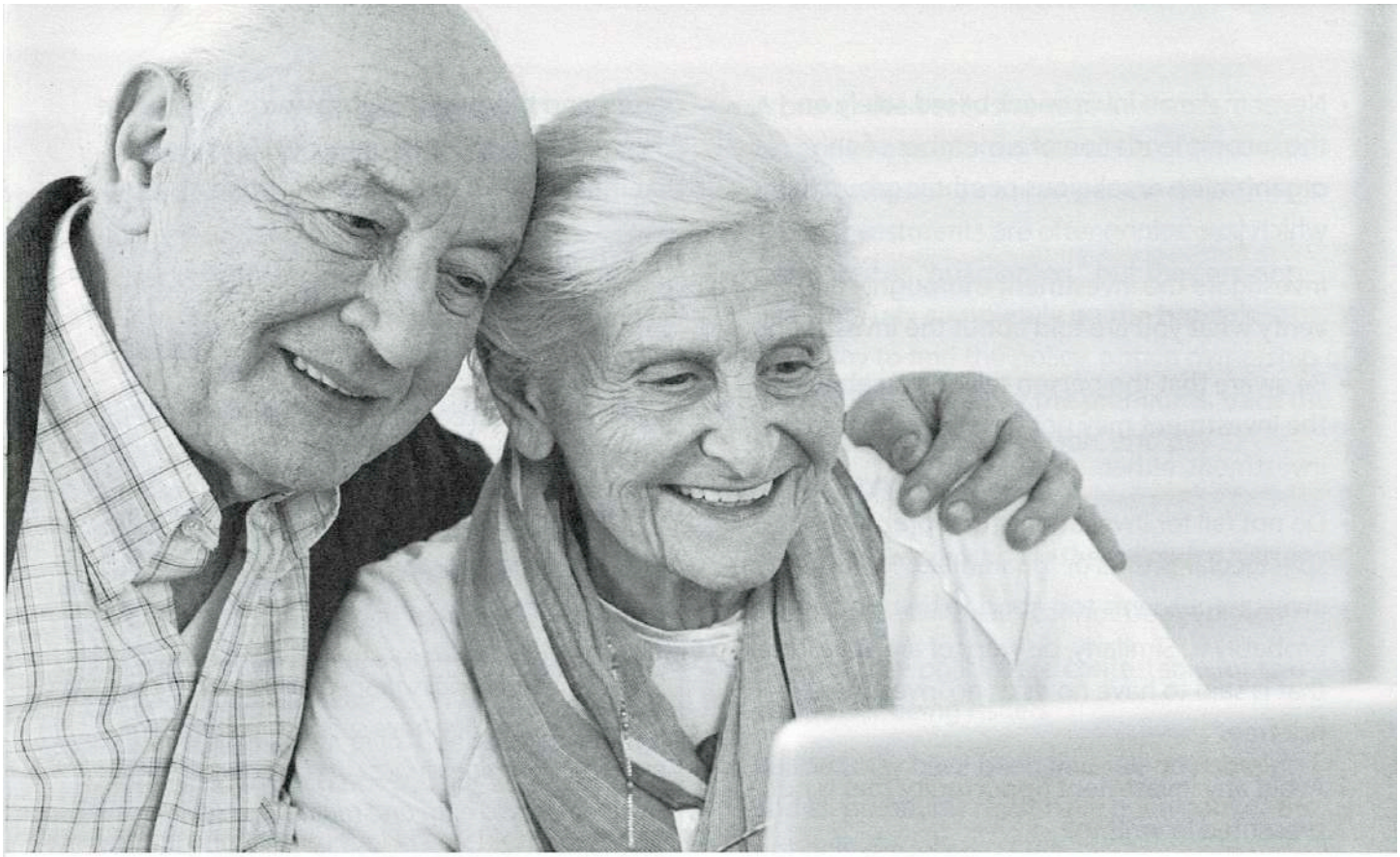
CALIFORNIA DEPARTMENT OF BUSINESS OVERSIGHT



PROTECT YOURSELF FROM FRAUD



Common Financial Frauds and Scams

The information and tips in this section are designed to help you become an informed investor and can help you, your family and your community recognize common frauds and scams.

Affinity Marketing and Affinity Fraud

Affinity fraud refers to investment scams that prey upon members of identifiable groups, such as religious or ethnic communities, the elderly, or professional associations. The people who promote affinity scams frequently are, or pretend to be, members of the association. They often enlist respected community or religious leaders from within the association to spread the word about the scheme by convincing them that a fraudulent investment is legitimate and worthwhile. Investing always involves some degree of risk. Minimize your risk by asking questions and getting the facts about any investment before you buy.

To avoid affinity fraud:

- No matter how trustworthy the person who brings the investment opportunity to your attention seems, verify everything.

- Never make an investment based solely on the recommendation of a member of an organization or religious or ethnic group to which you belong.
- Investigate the investment thoroughly and verify what you are told about the investment.
- Be aware that the person telling you about the investment may not have investigated the investment, either.
- Do not fall for investments that promise spectacular profits or "guaranteed" returns. If an investment seems too good to be true, then it probably is. Similarly, be wary of any investment that is said to have no risks; no investment is risk-free.
- Avoid any investment opportunity that is not presented in writing.
- Be suspicious if you are told to keep the investment opportunity confidential.
- Consult with an uninterested third party (such as an attorney or licensed financial planner or advisor) before you sign anything.

"Ponzi" and "Pyramid" Schemes These investments are illegal.

Many affinity fraud scams involve Ponzi or pyramid schemes, in which new investor money is used to make payments to earlier investors to give the illusion that the investment is successful. This ploy is used to trick new investors to invest in the scheme and to lull existing investors into believing their investments are safe and secure. In reality, the fraudster almost always steals investors' money for personal use.

Both types of schemes depend on an unending supply of new investors - when the inevitable occurs, and the supply of investors dries up, the whole scheme collapses and investors discover that most or all of their money is gone.

Be Suspicious if...

- Each new recruit must make an up-front investment or purchase a starter kit to join
- New recruits are required to purchase more products than they can reasonably sell
- Participants make money on each new recruit
- There is no customer refund policy

TIP

Sometimes financial salespeople will try to create the impression they have special credentials or expertise in senior services and products. The requirements to earn and maintain a senior designation vary considerably. If sales person's credentials contain words like "senior" or "elder" in conjunction with "certified" or "registered," proceed cautiously.

"Free Lunch" Seminars

Seniors frequently are invited to seminars that offer a free meal and information about investment opportunities, insurance products or wills and trusts. Free-meal seminars are rarely about education. Their ultimate goal is to recruit new clients and sell products. They may try to sell you unsuitable investments or convince you to replace your existing investments. They may not disclose their fees and commissions or other pertinent information, making it difficult to accurately compare products and services. Worse, some events are just a ploy to obtain your personal and financial information.

Also, be wary of so-called "experts" who misrepresent their qualifications. See Financial Industry Regulatory Authority (FINRA) on page 7 under "Helpful Resources" to check certifications.

Annuity Abuse

An annuity is a contract in which an insurance company makes a series of payments to you at regular intervals in return for a premium. Annuities are often purchased for future retirement income. As an annuity is a complex contract, it is important to know whether it fits your situation before signing a contract. For some, an annuity can be an appropriate part of an overall financial plan. Consider your goals, as well as how much risk you are willing to take.

Some annuity products carry high surrender fees. California requires individual annuity contracts for seniors to contain a disclosure regarding the surrender charge period. Ask about the drawbacks, not just the benefits. It also helps to talk to individuals with your interests in mind, such as a financial planner and/or tax consultant, before making a decision.

If you think you have been a victim of this type of abuse, see page 24 to contact the California Department of Insurance for more information or to file a complaint.

Viatical and Life Settlement Investments

Two legal, but highly risky investments, involve terminally ill or elderly people who sell the death benefit of their life insurance policy at a discount for cash. These people may accept cash to take out a new life insurance policy in their own name, based on their health and age. A broker then sells shares to investors, each to receive a proportionate share of the death benefit when the insured person dies. These investments are often erroneously promoted as "guaranteed," but they are not. Investors rely completely on the broker's company to find the policy, obtain ownership of the death benefit, pay the premiums, track the status of the insured person, and pay off the investment.

Risk is also increased for the following reasons:

- Precise dates of death cannot be predicted
- All insurance policies are contestable for two years after being issued
- Policies may have been fraudulently obtained, and all premiums must have been paid or the policy is cancelled
- Most companies have no proven track record of paying premiums or actually paying off on the investments when they become due.
- Other investment offers related to anticipated cash windfalls or future settlements (for example, insurance settlements, inheritances, or lottery winnings) pose similar high risks.

If you have been approached and asked if a policy can be taken out on you, or you wish to discuss another insurance matter, contact the California Department of Insurance.

Commodities Fraud

Be wary of any firm or individual offering to sell you commodity futures or options on commodities, including precious metals, such as silver or gold; foreign currency, such as Euros or Yen; energy resources like crude oil, heating oil, unleaded gas; or agricultural products such as corn or soybeans. Investing in commodities

is very risky and even experienced investors can lose their entire investment very quickly. Anyone who claims otherwise might be breaking the law. Always ask for proof and report fraud to the California Department of Business Oversight.

Promissory Note Fraud

Some promissory notes can be legitimate investments, while others turn out to be fraudulent. Salespeople offering promissory notes must be registered with the Department to sell securities.

A promissory note is a form of debt that companies sometimes use, like loans, to generate revenue. The company promises to return the buyer's funds (principal), and to make fixed interest payments in exchange for borrowing the money. Promissory notes have set terms, or repayment periods, ranging from a few months to several years. Investors who consider buying promissory notes should research them thoroughly. Contact the Department to verify whether the seller is properly licensed and in compliance with California's securities laws.

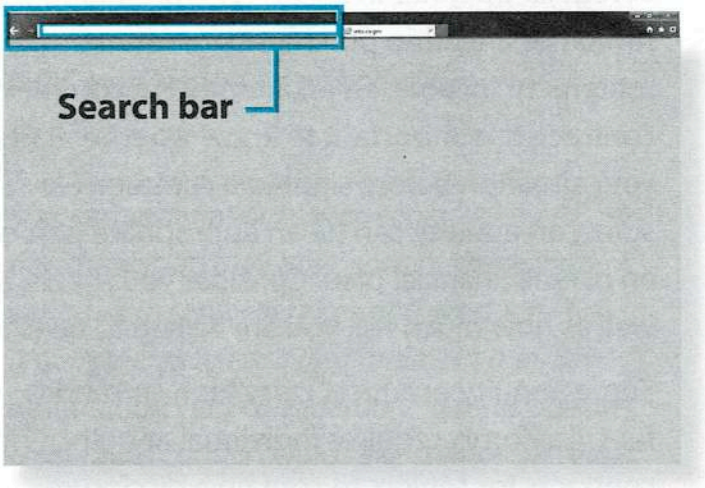
Online Escrow Scams

Carefully evaluate online escrow sites before signing up for any service. Many are phony copycat sites.

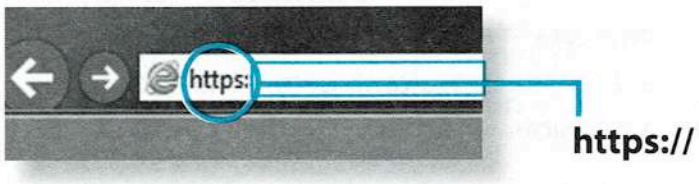
- Avoid any escrow service that does not list an address or phone number on their website - this is a red flag.
- Do not give personal or financial information over the Internet, unless it is via a secure website and you initiated the contact.

Secure sites have an "s" at the end of the "http" in their website address, displayed as "https." Most browsers display a padlock icon to indicate that the website is secure.

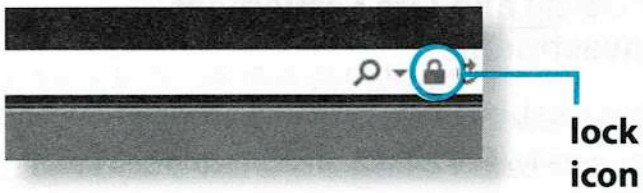
Browser window with search bar in top left of the screen:



Left side of search bar:



Right side of search bar:



Abusive Mortgage Lending Practices and Fraud

There are a wide array of abusive lending practices that impact borrowers with poor credit. Even consumers with credit in good standing may feel pressured to accept the terms offered or risk losing the opportunity to purchase a home they want very much. Abusive mortgage lending practices can include these activities:

- Frequent refinancing, or loan "flipping," that results in little or no economic benefit to the borrower and is undertaken with the primary objective of generating additional loan fees, prepayment penalties, and fees from the financing of credit-related products.
- Refinancing of special subsidized mortgages that result in the loss of beneficial loan terms.
- Packing of excessive and sometimes hidden fees in the amount financed and/or undisclosed or excessive interest.
- Using loan terms or structures – such as negative amortization – to make it more difficult or impossible for borrowers to reduce or repay their debt.
- Using balloon payments to conceal the true burden of the financing and to force borrowers into costly refinancing transactions or foreclosures.
- No-cost or low-cost (no out-of-pocket) prices to refinance. If it is too good to be true – then it is not really a deal. The cost is included somewhere in the loan, perhaps in a higher interest rate.
- Solicitations to repair consumers' credit by refinancing – consumers are advised to talk to a credit counselor before taking this step.
- Pressuring consumers into signing loans they cannot afford or do not understand.
- Convincing consumers to sign loan agreements without reading them.

Contact the Department to file a complaint about a mortgage company or salesperson, or for assistance to determine the appropriate governmental agency to contact.

Report Financial Fraud and Abuse

Do not let embarrassment or fear stop you from reporting fraud or abuse. If you have any doubts about an investment, or feel that you may have been a victim of fraud, please report such concerns immediately to the Department. Protect yourself and help protect others from fraud!

Check Before You Invest

Before engaging in financial or legal business, ask the salesperson to complete the "Check Before You Invest" form located on page 23 and then contact the Department toll-free 1-866-275-2677 or go to our website www.dbo.ca.gov to verify the license.

Remember...

When making a financial decision, be sure to evaluate all of your options and compare fees and services. Contact the California Department of Business Oversight (or the appropriate licensing agency) to check the license status of any financial professional before you make a final decision. To check the license of a real estate broker, contact the California Bureau of Real Estate toll-free 1-877-373-4542 or visit their website at www.bre.ca.gov.

TimeShare Scams

Con artists are known to perpetuate a scam that begins with obtaining identities of timeshare owners from public records.
They call the owners claiming to have clients who are interested in purchasing their timeshare, explaining that the owners need to pay a fee before the transaction can proceed. If the first fee is paid, a second fee is requested and the scam continues as long as the timeshare owner continues to pay.

The use of phony California escrow companies has become part of this pitch. Scammers use the names of inactive and active licensed escrow companies and then create phony websites in those names. The scammers are using the names of the people who were actually involved in the defunct companies and claiming to be legitimately licensed. Before you proceed, contact the California Department of Business Oversight to verify an escrow licensee and report anything suspicious.

Charity Scams

Con artists often try to take advantage of the generosity of others, especially after a well-publicized disaster such as a hurricane or fire. Be wary of any solicitations from charities you don't already know, as well as those you do. Verify that a charity is legitimate before sending them a check or providing your credit card number. To become better informed about a charity before making a donation, visit the California Office of Attorney General's website www.oag.ca.gov.

Grandparent Scams

In this scam, a grandparent receives a call from an imposter claiming they are related (usually as a grandchild), in trouble and urgently request they send money. The imposter describes various versions of an emergency. Their stories have included traveling in another country, being arrested, in the hospital, a car accident and/or needing emergency car repair.

The imposter sounds distressed and may be calling from a noisy location and claim they only a few moments to talk. Sometimes another person comes on the line identified as a lawyer or the arresting officer to add credibility to the story. The grandchild-imposter asks the grandparent to immediately wire money and not to tell anyone. The scammer typically asks for several thousand dollars and may even call back again several hours or days later asking for more money to be wired or to provide bank account routing numbers. Always verify the legitimacy of the call before sending money to anyone! Once the money is wired, it is nearly impossible to recover.

Lotteries and Sweepstakes Scams

Scam artists often use the promise of a valuable prize or award to entice people to send money. Victims receive a letter, an email or text message claiming they have won a foreign lottery or a sweepstakes. Scammers tell victims to claim their prize by sending a personal check, money order or wire transfer to cover taxes, fees, shipping costs, or insurance.

It is illegal for a U.S. resident to play a foreign lottery. Any letter or email from a lottery or sweepstakes that asks you to pay taxes, fees, shipping, or insurance to claim your prize is also illegal.

Foreign Letter Scams

If you receive a letter claiming to be from Nigeria or another foreign government, foreign official, widow or service member asking you to send personal or bank account information, do not reply in any manner. Be skeptical of individuals representing themselves as foreign government officials asking for your help in placing large sums of money in overseas bank accounts. Do not believe the promise of large sums of money for your cooperation. Always guard your account information carefully.

Phishing Scams

Phishing is an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites such as government entities, banks and credit unions, as well as many popular retailers – and even friends and family members.

Other Helpful Resources:

The U.S. Securities Exchange Commission (SEC) Office of Investor Education and Advocacy provides a variety of services and tools to help investors invest wisely and avoid fraud. Visit www.investor.gov or www.sec.gov or call toll-free 1-800-732-0330.

Contact the Financial Industry Regulatory Authority (FINRA) to check a broker or investment adviser background. Go to FINRA BrokerCheck at www.finra.org or call toll-free hotline 1-800-289-9999.

The Federal Trade Commission (FTC) warns users to be suspicious of any official-looking email message that asks for updates on personal or financial information. Recipients should go directly to the organization's website to find out whether the request is legitimate. If you suspect you have been phished, forward the email to spam@uce.gov or call the FTC toll-free helpline 1-877-FTC-HELP (1-877-438-4338).