The 1st Judicial District Attorney's Office in conjunction with

Community Partners

to provide fraud prevention, intervention, and victim support.

1st Judicial District - District Attorney Fraud Line

303-271-6980

"This project was supported by Grant No. 2011-DJ-BX-0316 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in the document are those of the author and do not represent the official position or policies of the United States Department of Justice."

TEST YOUR 'FRAUD IQ'

TRUE OR FALSE?

1. **The top ways identity thieves get your info is through purse snatching, mail theft, dumpster diving and e-mail "phishing."**

2. **It's a good idea to carry your Social Security card with you.**

3. **Once you have subscribed to the Colorado "No Call" list, you do not have to worry about telemarketers.**

4. **There is a law that requires charities to spend a certain percentage of their income on programs and services.**

5. **Foreign lotteries are illegal in the U.S.**

6. **As long as you don't buy any magazines or send any money, playing sweepstakes is harmless entertainment.**

7. **Colorado has a state contractor's licensing board that licenses and approves contractors.**

8. **If a uniformed utility employee appears at your door to conduct an inspection, shows a badge and ID, it's safe to invite him in.**

9. **Most investment fraud is perpetrated by long term, trusted advisors.**

10. **If you have a trusted family member, a financial advisor, or someone with your Power of Attorney who is paying your bills and managing your money, it is critical that you review your account statements.**

FRAUD QUIZ ANSWERS

1. *TRUE* **True, thieves are everywhere – even churches – looking to steal purses and the checkbooks, credit cards and other info they find inside. They are also looking for checks, pre-approved credit card applications, and account statements in your mail box. They rummage through trash looking for unshredded info containing account numbers. And they send "phishy" e-mail asking you to verify account numbers by impersonating your bank, credit card company, government agency, etc.**

2. *FALSE* **It's a good idea to have nothing in your purse or wallet that contains your Social Security number. An identity thief can apply for and receive credit in your name: credit cards, loans, gambling credit, cars, etc.**

3. *FALSE* **Although consumers who have subscribed to the Colorado No Call List have reported a strong decrease in calls, there are exemptions, including non-profit and charitable organizations, politicians, and those with whom you have an established business relationship, such as phone companies. The No Call List will not stop criminal telemarketers – to protect yourself, simply do not talk to strangers!**

4. *FALSE* **It is the donor's responsibility to determine how his or her donations are used. Ask charities for a copy of their annual report and contact the BBB's Wise Giving Alliance at www.give.org or 303-222-4444.**

5. *TRUE* **Federal law prohibits mailing payments to purchase any ticket, share or chance in any foreign lottery. Telemarketing con artists from Canada have conned hundreds of Coloradans into sending millions in payments for "taxes" before collecting on their bogus Canadian lottery winnings**

6. *FALSE* **When you play sweepstakes, your name is frequently put on marketing lists bought and sold by other direct marketers. Eventually, your name can end up on criminal telemarketing lists.**

7. *FALSE* **Colorado is one of a few states that does not require statewide regulation of all contractors. Consumers have a greater responsibility to protect themselves from contractor fraud.**

8. *FALSE* **City and utility workers do not go door-to-door; but con artists do! Once in your home, he will distract you while an accomplice sneaks in to steal purses, jewelry, safes, and other valuables. *Never* let a stranger in your home – no matter who they claim to be!**

9. *TRUE* **The vast majority of investment fraud cases prosecuted by the District Attorney's Office involve financial advisors who have had long-term, trusting relationships with their victims. The perpetrators use trust – and sometimes faith – as their weapons. No matter how long you've known or trusted someone, never make an investment decision without seeking advice from a lawyer, accountant, and/or the Colorado Division of Securities.**

10. *TRUE* **In all cases of theft by family members, trusted advisors, and Powers of Attorney, victims have given up total control to others and did not review financial statements. Perpetrators took advantage of the victims' trust. In addition to your own review of accounts, surround yourself with several advisors and caregivers who can provide a system of checks and balances so that no one person has total control over your finances.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

SEVEN PREDOMINANT AREAS OF FRAUD

Identity Theft

Warning Signs:

- ⇨ **Your purse or wallet is stolen**
- ⇨ **Your bank account is overdrawn or there is unusual activity on your credit card**
- ⇨ **Mail you are expecting doesn't arrive, especially related to financial matters; bills you paid are still showing due**
- ⇨ **You apply for a credit card or loan and are denied**

Preventative Steps:

- **Carry a close-fitting pouch instead of a purse or carry a wallet in your front pocket.**
- **Reduce the items you carry in public such as extra credit cards, Social Security card, and checkbooks; remove your Social Security number from your Driver's License.**
- **Shred, tear into small pieces, or cut up all mail and documents that contain Social Security, bank and credit card numbers.**
- **Place mail with bills to be paid at the Post Office. Ask that new boxes of checks be held at your bank or credit union rather than mailed to you.**

To Report Fraud: 303-271-6980

You will reach a live person!

TELEMARKETING FRAUD

Warning Signs:

- **You live alone and enjoy talking to anyone calling**
- **You believe it's rude to interrupt a caller or to hang up**
- **You must pay money up front for taxes or fees to participate**
- **You must make an immediate decision, before the call ends, or the offer will be rescinded**
- **You are called more and more frequently by a multiplying variety of telephone solicitors**

Preventative Steps:

- **Never talk to strangers on the telephone – they are not calling to wish you a good day. They are invading *your* privacy – as though they have walked into your home.**
- **Use an answering machine, voice mail or *Caller ID* to screen calls.**
- **Never, under any circumstances, give any portion of your credit card, bank account, or Social Security numbers to a caller.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

MAIL AND INTERNET FRAUD

Warning Signs:

- **You play sweepstakes daily because you think you need extra money, holding out hope you will win a big prize some day**
- **You believe because your mail is delivered by the U.S. Postal Service, it must be legitimate**
- **You open and read all of your mail because many pieces look like official government documents or heart-felt solicitations for charity – and you don't have anything better to do**
- **You're getting the same offers through e-mail that you used to receive through the mail**

Preventative Steps:

- **Even though it may be fun or give you something to do, stop participating in sweepstakes, lottery, and contest offers.**
- **If you were to truly win something, you NEVER have to pay any fees, taxes, or costs of ANY kind before receiving your winnings – that's the law!**
- **Don't even give temptation a chance. If you receive a mailing or e-mail that promotes sweepstakes, lotteries, charities, credit repair, work-at-home offers, or a Nigerian letter, throw the envelope away or delete the e-mail without opening it.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

You will reach a live person!

CONTRACTOR FRAUD

Warning Signs:

- **A home repair contractor solicits you at your door, insisting you have a problem which must be repaired right away**
- **A contractor offers a bargain price or claims to have materials left over from another job**
- **A contractor requires a substantial payment in advance or charges significantly more after the work is completed**
- **An inspector appears at your door, claiming to work for the city or a utility company and must come into your home to inspect your water heater, furnace, or back yard**

Preventative Steps:

- **BEWARE door-to-door contractors who use high-pressure or scare tactics to get an immediate decision.**
- **DON'T do business with someone who comes to your door offering a bargain or claims to have materials left over.**
- **Get at least 3 written bids. DON'T always choose the lowest bidder– almost all complaints to the District Attorney's Office are contractors with very low bids. You get what you pay for!**
- **Require the contractor to use a written contract that lists materials, costs, and the completion date.**
- **Don't allow any stranger into your home, no matter who they claim to be. City inspectors do not go door to door!**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

Mortgage and Quit Claim Deed Scams

Warning Signs:

- **You've fallen behind in your mortgage payments or you are already in foreclosure**
- **You're getting phone calls and visits from companies offering to help you pay off your debts**
- **You're receiving numerous fliers in the mail or on your door offering low interest cash loans**
- **A friend, advisor or relative asks you to sign some forms – you do, without reading them**

Preventative Steps:

- **Beware of companies who contact you in person or by fliers offering a foreclosure relief service.**
- **Don't sign any forms or papers without reading and understanding what you're signing. If you're uneasy or feeling pressured, get advice from a lawyer or other advisor.**
- **Don't deed your property to *anyone*. First consult an attorney, a knowledgeable family member, or someone else you trust completely. Once you sign legal papers, it can be difficult, or even impossible, to reverse the action.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

You will reach a live person!

Financial Planning and Investment Fraud

Warning Signs:

- **High pressure sales tactics with an insistence on an immediate decision;**
- **Unwillingness to let you discuss the deal with another advisor or to get a second opinion;**
- **A guaranteed investment or one with 'no risk';**
- **Unwillingness to provide written information, including state securities registrations and verifiable references;**
- **A suggestion that you invest on the basis of trust or faith.**

Preventative Steps:

- **Surround yourself with several advisors – don't become solely dependent on one financial advisor or consultant.**
- **Thoroughly check out any offer – don't be rushed into making a hasty decision. Contact the Colorado Division of Securities at 303-894-2320 if you have questions.**
- **Carefully review your financial statements and look for signs of unauthorized or excessive trading. Periodically check your account online or by phone with the fund managers.**
- **If you have trouble retrieving your funds, don't let a false sense of trust keep you from demanding a return of your investment.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

CAREGIVER FRAUD

Warning Signs:

- **Unusual activity in bank and credit card accounts**
- **Caregiver tries to isolate the victim who comes to rely solely on the caregiver**
- **Caregiver has total control over finances and has all financial statements mailed to him or her.**
- **New acquaintances appear on the scene and the adult is either completely charmed, or fearful of the caregiver**

Preventative Steps:

- **If your Power of Attorney or anyone else suggests you make a change in your assets, your investments, or insurance, always get two or three other opinions from within your team of advisors. Only a potential crook will not want you to discuss the change with others.**
- **No matter how much you know, love or trust someone, never sign papers you have not read or do not understand.**
- **Even if you have a representative payee, Power of Attorney or other advisor who manages your finances, insist on receiving and reviewing copies of all bank and financial statements.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

You will reach a live person!

Power Against Fraud Action Tips

FRAUD PREVENTION CHECKLIST

- ☐ **Use a 'fanny pack' or close-fitting pouch, instead of a purse or wallet any time you are out in public.**
- ☐ **Do not carry your Social Security card with you, and remove your Social Security number from your Driver's License and checks.**
- ☐ **Deposit all outgoing mail at your Post Office rather than placing in your mailbox for carrier pick-up.**
- ☐ **Use a confetti/crosscut shredder on all financial mail and documents.**
- ☐ **Establish a policy of not talking to strangers on the telephone, at your door, or on the street.**
- ☐ **Sign up for the Colorado "NO CALL" list.**
- ☐ **Request those with whom you have established business relationships (phone companies, banks, credit card issuers) to put you on their "Do Not Call" and "Opt Out" lists.**
- ☐ **Send a letter to the Mail Preference Service to remove your name from marketing lists.**
- ☐ **Make an annual charitable giving plan and do not give to charities soliciting by telephone or door-to-door.**
- ☐ **Get three written bids before contracting for any home improvement and check out contractors with the Better Business Bureau and city building department.**
- ☐ **Contact an attorney to discuss a Living Will and Powers of Attorney, and to set up a system of checks and balances so that no one person has total control over your finances.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

ID Theft Prevention Checklist

☐ **Carry any document with sensitive information in a close fitting pouch or in your front pocket, not in your purse or wallet. Sensitive documents include driver's license, credit & debit cards, checks, car registration and anything with your Social Security Number.**

☐ **Don't carry your checkbook in public; carry only the checks you need.**

☐ **If possible remove anything from your wallet containing your SSN, including your Social Security card, Medicare card, military ID card. If your SSN is on your Driver's License – get a new license.**

☐ **Don't give any part of your Social Security number, credit card or bank account numbers over the phone, e-mail or Internet, unless you have initiated the contact to a verifiable company or financial institution.**

☐ **Request a free copy of your credit report once a year.**

☐ **Notify the credit reporting agencies of the death of a relative or friend to block the misuse of the deceased person's credit.**

☐ **Call your bank and credit card customer service and ask to "opt out" of ALL marketing programs, including 'convenience' checks mailings.**

☐ **Call the Credit Card Offer Opt Out Line to reduce number of credit card solicitations you receive.**

☐ **Shred pre-approved credit card offers, convenience checks and any document containing sensitive information – with a crosscut shredder.**

☐ **Mail bills to be paid at the Post Office, not in your mailbox or in street corner postal boxes. Consider using automated payment plans.**

☐ **Ask your bank or credit union to receive your box of new checks, rather than have them mailed to your home.**

☐ **Do not keep your auto registration, insurance card, checkbook, receipts, or other identifying information in your car. Carry them in a secure manner on your person. Do not leave your car unlocked.**

☐ **Check your earnings record at least annually and more often if you suspect your SSN has been compromised (it's free and there is no limit to how often you may request it.) Contact the Social Security Administration (see page 8, Item 4) and ask for Form SSA-7004, *Request for Earnings and Benefit Estimate Statement*.**

COMPUTER PRECAUTIONS

☐ **Never respond to e-mails requesting personal information such as bank or charge account numbers; Social Security numbers; pin numbers/passwords. This rule applies even if the sender appears to be your bank or credit card company; a government agency such as the Federal Deposit Insurance Corporation, Social Security Administration, or IRS; or companies such as AOL, Ebay, PayPal, etc. No legitimate company/agency will send an e-mail asking you to verify information.**

☐ **Delete unknown or questionable e-mails without opening.**

☐ **Use a firewall program, especially if you use a high-speed connection like cable, DSL or T-1, which connects your computer 24 hours a day. The firewall program allows you to stop uninvited guests from accessing your computer. Without it, hackers can take over your computer, access personal information stored on it, or use your computer to commit crimes.**

☐ **Use a secure browser – software that encrypts or scrambles information you send over the Internet – to guard the security of online transactions. Be sure your browser has up-to-date encryption capabilities by using the latest version available from the manufacturer. When submitting information, look for the "lock" icon or "https" on the browser's status bar to ensure your information is secure during transmission.**

Remove Your Name From Marketing Lists

- ☐ **1. Don't play direct mail sweepstakes or talk to telemarketers.**
- ☐ **2. Sign up for the Colorado "No Call" List for both your home and cell phones at 1-800-309-7041 or 303-776-2678 or www.coloradonocall.com.**
- ☐ **3. Call phone companies, and others with whom you do business and ask that they put you on their "DO NOT CALL LISTS."**
- ☐ **4. Call the credit reporting agencies' "OPT OUT LINE" to get off mailing lists for unsolicited credit card offers: 1-888-567-8688 or www.optoutprescreen.com.**
- ☐ **5. Call the customer service numbers for your credit card (s) and ask to "OPT OUT" of marketing programs, including "convenience checks."**
- ☐ **6. Opt out of e-mail and direct mail by contacting the Direct Marketing Association. At: www.dmachoice.org (Free) or by sending the letter on the next page ($1 Fee).**
- ☐ **7. Reduce mortgage and real estate solicitations by OPTING OUT of lists collected and sold by Acxiom by calling 1-877-774-2094 or E-mailing optoutUS@acxiom.com. It is not necessary if you OPT OUT of the Direct Marketing Association mailing lists (see above).**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

Mail Preference Service
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512

To Whom It Concerns:

Please remove my name from your marketing lists. Thank you for your attention to this matter. My name and address are:

All versions of your name
used in mailings
Your Mailing Address
City, State, Zip Code

SIGN YOUR NAME

(INCLUDE $1.00)

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

Tips To Stop Unwanted Calls

Keep this script near your telephone. If you are contacted by a telemarketer or someone soliciting contributions, read from the script and hang up when you have finished reading.

I do not do business over the telephone.
(I do not donate to charities over the telephone.)
Please put me on your "DO NOT CALL" list.
Thank you.

The District Attorney's Suggestion

Do not allow the caller to interrupt you or try and get you to stay on the line by trying to engage you in further talk. Read the script and hang up. This is NOT BEING RUDE. It is protecting you from unwanted, and perhaps criminal, offers and intrusions.

If telemarketers call you back or are rude, interrupt and say:
"We don't have a good connection – call me back on my other line."
Give them the Jefferson/Gilpin DA's Fraud Hot Line Number

303-271-6980

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

Annual Charitable Giving Plan

Name of Charity	Annual Gift
1. _____	_____
2. _____	_____
3. _____	_____
4. _____	_____
5. _____	_____
Total Annual Charitable Giving Budget	_____

☐ **I have asked for, and received, written information, such as an Annual Report, from each charity.**

☐ **I have checked out these charities through the Better Business Bureau Wise Giving Alliance: www.give.org or 303-222-4444, or through charitynavigator.org**

☐ **If solicited by telephone or in person for a charitable donation, I will respond *"I already have a chosen list of charities I support! If you would like me to consider you for next year, please send me your annual report."***

☐ **I will not change my charitable giving list without checking out any new charity to which I may consider giving.**

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

ARRANGE FOR A CREDIT FILE

SECURITY FREEZE

Coloradoans can put a security freeze on their credit reports. A freeze means your file cannot be shared with potential creditors which can help prevent identity theft. If your files are frozen, even someone who has your name and Social Security number will not be able to get credit in your name.

To place a security freeze:

Send a request in writing by Certified Mail to each of the three major consumer credit reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA. 30348	Allen, TX. 75013	Fullerton, CA. 92834

Include the following in your request:

- Full name, with middle initial and generation, such as Jr., Sr., II;
- Social Security number;
- Date of birth;
- Current address and previous addresses for the past two years;
- Copy of a government issued ID, such as a driver's license or military ID;
- Copy of a utility bill, bank or insurance statement that displays your name, current mailing address, and date of issue (statement date must be recent).

The initial freeze is free of charge; however, the temporary or permanent removal of the freeze may cost up to $10 per agency. To allow a "Background Check" by a potential employer or to apply for new credit, the freeze would need to be lifted.

From the Office of the 1ST District Attorney
To Report Fraud: 303-271-6980

You will reach a live person!

RESOURCES

IMPORTANT RESOURCES

♦ *District Attorneys' Office*

To report suspected fraud, or if you need assistance in reporting a crime or think you or someone you know is being victimized, call:

Jefferson/Gilpin Economic Crime Specialists

Deb Ohno	**303-271-6931**	**dohno@jeffco.us**
Cary Johnson	**303-271-6970**	**csjohnso@jeffco.us**

♦ *Colorado "No Call" List*

Sign up for the Colorado telemarketing "NO CALL" list by making one telephone call. Exceptions to the "No Call" law are charities, politicians, and companies with whom you have an established business relationship. The call is free and there is no charge.

1-800-309-7041 or 303-776-2678 or www.coloradonocall.com

♦ *Credit Card Offer "Opt Out" Line*

To stop credit card offers or unwanted credit cards, call the "OPT OUT LINE." The call is free and there is no charge for this service. You will need to give your Social Security Number.

1-888-567-8688 or www.optoutprescreen.com

♦ *Business and Charity Reliability Reports*

To receive a reliability report on a business or charity, contact the Better Business Bureau:

303-222-4444 or www.denver.bbb.org and www.give.org.

You can also contact Charity Navigator: www.charitynavigator.org.

♦ *Investment Offers*

To inquire about the legitimacy of any investment offer that you don't understand or that seems unusual, call the Colorado Division of Securities. Make this call before you invest any money.

303-894-2320

♦ *Credit Reporting Agencies*

To receive a FREE copy of your Credit Report, making sure there is no inaccurate information or unusual activity, contact the following. You will need to give your Social Security Number.

Equifax
To order your report, **www.annualcreditreport.com**
Call: **800-685-1111** or write: **P.O. Box 740241, Atlanta, GA 30374-0241**

To report fraud, call: **800-525-6285** and write:
P.O. Box 740241, Atlanta, GA 30374-0241

Experian
To order your report, **www.annualcreditreport.com**
Call: **888-EXPERIAN (397-3742)** or write: **P.O. Box 2002, Allen TX 75013**

To report fraud, call: **888-EXPERIAN (397-3742)** and write:
P.O. Box 9530, Allen TX 75013

Trans Union
To order your report, **www.annualcreditreport.com**
call: **800-888-4213** or write: **P.O. Box 1000, Chester, PA 19022:**

To report fraud, call: **800-680-7289** and write:
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

Five Red Flags of Fraudulent Scams

The scams and fraudulent schemes that come to consumers, via E-mail, phone calls, and the U.S. Postal Service change all of the time. It could be the 'Grandparent' scheme, an offer to reduce credit card interest rates, the offer to sell a TimeShare, the opportunity to be a Trade Representative for a foreign company wanting to do business in the United States, or simply the announcement of winning a lottery or prize. The wise approach is to look for commonalities that are included in these schemes. Then, no matter what the approach or offer coming today, you can identify the 'Red Flags' that mark it as fraudulent.

Red Flag #1: **They contacted you; you did not contact them!**

The E-mail, phone call, or mailed letter came out of the clear blue. Always check out issues by obtaining the phone number of the agency or business making the offer and YOU CALL THEM! Do not call the number they provide in an E-mail or letter.

Red Flag #2: **They want the issue or offer to remain secret and confidential.**

You are to tell no one about the offer, prize, or steps you need to follow for the offer to come to fruition.

Red Flag #3: **You must act with urgency and immediacy!**

This is, quite frankly, an attempt to get you to act before you think things through carefully. While the adrenaline is flowing from your excitement over a windfall, one which isn't true, they want you to call or send money.

Red Flag #4: **"If it sounds too good to be true, it is too good to be true."**

This was true 50 years ago. It still is true!

Red Flag #5: **You will need to wire money or send money using something like a 'Green Dot' money card.**

Money that is wired or sent using a money card is, most likely, heading to a crook overseas. Once sent, it is probably gone forever.

To schedule a "Power Against Fraud" crime prevention program for your group or agency, please contact:

Cary Johnson
Director: Power Against Fraud
Crime Prevention Programs
District Attorney's Office
303-271-6970
csjohnso@Jeffco.us

District Attorney's Website:

www.Jeffco.us/da

We are grateful for the generous support provided by FirstBank