STAND UP AGAINST FRAUD

BETH MCCANN DENVER DISTRICT ATTORNEY

PACKET PROVIDED BY THE

DENVER DISTRICT ATTORNEY'S OFFICE

What is Your ID Theft Probability Score?

1. I pay bills with checks and place them in my mailbox or in a corner postal box. **__10 points**

2. I do not use direct deposit or electronic transfer for paychecks, refund or insurance claims checks. **__ 5 points**

3. New boxes of checks are mailed to my home. **__ 10 points**

4. I have not 'opted out' of my credit card marketing programs and receive "convenience" checks in the mail. **__ 10 points**

5. I carry a purse or wear a wallet in my back pocket. **__ 10 points**

6. I use checks for shopping and carry my checkbook with me when in public. **__ 5 points**

7. I have not copied the contents of my wallet. **__ 5 points**

8. I have at least one item in my wallet that contains my SSN. **__ 10 points**

9. I throw away my annual Social Security Earnings Statement without reviewing it **__ 10 points**

10. I keep my purse, briefcase, checkbook, registration, insurance card, or other identifying information in my car. **__ 10 points**

11. I do not keep financial and personal documents in locked files in my home or office. **__ 10 points**

12. I do not shred bank/credit info before trashing. **__ 10 points**

13. I use a shredder, but not a cross-cut shredder. **__ 5 points**

14. I have not "opted out" of credit reporting agencies' credit card solicitations. (1-888-567-8688 or www.optoutprescreen.com)
__5 points

15. I have not ordered copies of my credit report in over a year.
__10 points

16. I have not notified the credit reporting agencies of the death of a relative or friend. **__10 points**

17. I have responded to e-mails or telephone calls from my Internet provider, bank, or companies like eBay or PayPal requesting account verification ("phishing'). **__10 points**

18. I use e-commerce, but do not use a secure browser, or I have high-speed internet service but no firewall protection.
__10 points

MY ITP SCORE _____

SCORING

- **60+ points** - You are at high risk of being an ID theft victim. We recommend you use the attached check list to reduce your vulnerability.

- **30-60 points** - Your odds of being victimized are about average. Higher if you have good credit. Use the attached check list to identify additional changes that will reduce your risk.

- **0-30 points** - Congratulations. You have a high "IQ." Keep up the good work, but check the attached list for anything you may have overlooked.

10 Ways to Avoid Fraud

Crooks use clever schemes to defraud millions of people every year. They often combine new technology with old tricks to get people to send money or give out personal information. Here are some practical tips to help you stay a step ahead.

1. **Spot imposters**. Scammers often pretend to be someone you trust, like a government official, a family member, a charity, or a company you do business with. Don't send money or give out personal information in response to an unexpected request — whether it comes as a text, a phone call, or an email.
2. **Do online searches**. Type a company or product name into your favorite search engine with words like "review," "complaint" or "scam." Or search for a phrase that describes your situation, like "IRS call." You can even search for phone numbers to see if other people have reported them as scams.
3. **Don't believe your caller ID**. Technology makes it easy for scammers to fake caller ID information, so the name and number you see aren't always real. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back to a number you know is genuine.
4. **Don't pay upfront for a promise.** Someone might ask you to pay in advance for things like debt relief, credit and loan offers, mortgage assistance, or a job. They might even say you've won a prize, but first you have to pay taxes or fees. If you do, they will probably take the money and disappear.
5. **Consider how you pay.** Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money through services like Western Union or MoneyGram is **risky** because it's nearly impossible to get your money back. That's also true for reloadable cards like MoneyPak, Reloadit or Vanilla. Government offices and honest companies won't require you to use these payment methods. Be cautious if someone requests payment via one of these methods.
6. **Talk to someone.** Before you give up your money or personal information, talk to someone you trust. Con artists want you to make decisions in a hurry. They might even threaten you. Slow down, check out the story, do an online search, consult an expert — or just tell a friend.
7. **Hang up on robocalls.** If you answer the phone and hear a recorded sales pitch, hang up and report it to the FTC. These calls are illegal, and often the

products are bogus. Don't press 1 to speak to a person or to be taken off the list. That could lead to more calls.

8. **Be skeptical about free trial offers.** Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. And always review your monthly statements for charges you don't recognize.
9. **Don't deposit a check and wire money back.** By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. If a check you deposit turns out to be a fake, you're responsible for repaying the bank.
10. **Research.** Get at least 3 bids on all work including small jobs like tree trimming, car repair, even gardening. Hiring the first person that comes to your door or sends a solicitation letter, can result in shoddy or unfinished work.

Colorado ranked No. 13 for per-capita identity theft complaints to the Federal Trade Commission in 2014, according to a recent report released by the commission.

Reduce Your ID Theft Risk

- Mail paid bills at the Post Office, not your mailbox or in street corner postal boxes. Consider using automated payment plans, but do not 'save' your credit info on the website for ease later.
- Have paychecks, benefit and pension checks direct deposited to your account. Ask the IRS, insurance companies and others to send refund checks electronically.
- Ask your bank or credit union to receive your box of new checks, rather than have them mailed to your home.
- Call your bank and credit card customer service and ask to "opt out" of **ALL** marketing programs, including 'convenience' checks mailings.
- Carry sensitive information in a close-fitting pouch or in your front pocket, not in your purse or wallet, including driver's license, credit & debit cards, checks, car registration and anything with your Social Security Number (make a copy of your Medicare card and black out all but the last four digits.)
- Do not carry your checkbook in public. Carry only the checks you need.
- Copy the contents (back and front) of your wallet.
- 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.
- 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*.
- Do not keep your purse, briefcase, checkbook, registration, insurance card, or other identifying information in your car. Carry them in a secure manner on your person. Do not leave your car unlocked or unattended.
- Keep your financial and tax records in locked files in your home or office.
- Do not give any part of your Social Security, 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 the Credit Card Offer Opt Out Line to reduce number of credit card solicitations you receive. (1-888-567-8688 or www.optoutprescreen.com)
- Shred pre-approved credit card offers, convenience checks and any document containing sensitive information - with a crosscut shredder.
- Do not respond to e-mails asking to submit personal data. The message may include fancy graphics, trademark symbols and an authentic-looking e-mail address, but that can be faked. Here are ways to tell:
    - The message tries to scare you saying your account needs to be verified/updated.
    - The message threatens negative action if you fail to act immediately.
    - The message asks you to click on a link or to submit information through a button. Legitimate emails will not contain a link, but will ask you to close out the message, open the company's Internet Web site, and use your name and password to update the required information. Never click on a link provided in the message!
    - The message appears to come from a company with whom you do business, but it calls you "Dear Customer" instead of your name.
- Use a firewall program if you use a high-speed connection like cable, DSL or T-1, which connects your computer 24 hours a day. A firewall may stop hackers from accessing your computer. Without it, they can access personal information and use it 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.

5 RED FLAGS OF A SCAM

1. **FEAR**. If someone calls and your first reaction is “Oh No!”, then take heed. Scammers use fear as the number one method for getting you off your guard.
2. **Asks for “verification” of your personal information**. Is the person asking to “confirm” your full social security number, bank account number?
3. **Pay Up and Pay immediately**. Scammer will say “I can help you”, but you must pay now, over the phone.
4. **Requests payment in the form of a gift card**. No reputable company, no lawyer, not the IRS or Microsoft, requires you to go to a store and purchase some form of a gift card (could be from any store, Best Buy, Walgreens etc.); or an ITunes card, or some other sort of card.
5. Tells you to tell no one.

QUICK TIPS

1. **Never answer the phone if you do not recognize the number.** Scammers can make a phone number appear as a local number. The best way to reduce calls from unscrupulous telemarketers is not to answer the phone. Err on the side of someone leaving a message versus answering any calls.
2. **SHRED SHRED SHRED.** Any document, mailing label etc that has your name and address on it. Do not forget to shred those preapproved checks from your bank or Credit Card Company.
3. Copy all the contents of your wallet, front and back. It may not keep you from losing your wallet, but if it does get lost, you will have copies of all your lost items.
4. Do not have your checkbooks mailed to your home. Instead, pick them up at your bank.

IF YOUR IDENTITY'S STOLEN

Resolving the consequences of identity theft left to the victim. Act quickly and assertively, and keep records/copies of all contacts and reports

- File a report with the police/sheriff in the jurisdiction in which you live and get a copy of the report for the credit agencies, banks and credit card companies. File a "counter report" or file online. In Denver file at **www.denvergov.org/policereport**. You can also request and complete the *ID Theft Affidavi*t from the Federal Trade Commission (**www.ftc.gov**).

- Cancel each credit card. If you report the loss before the cards are used, you are not responsible for any unauthorized charges. Beware of callers selling credit card protection – you do not need this! Carefully monitor your credit card statements for evidence of fraudulent activity.

- Contact your financial institutions, cancel all accounts, and PIN numbers. Stop payments on outstanding checks and complete "affidavits of forgery" on unauthorized checks.

- Consider placing a **Security Freeze** on your credit file (see page 8) **OR**

- Report the theft to the fraud units of the credit reporting agencies. Request the credit reporting agencies to flag your credit file for fraud. Add a victim's statement to your report: **"My identification has been used to apply for fraudulent credit. Contact me at (your telephone number or address) to verify ALL applications."**

- Consider subscribing to a credit report monitoring service (available from the credit reporting agencies) that includes fraud-watch e-mails and frequent credit reports.

- Ask utility companies (especially cellular service) to watch for anyone ordering services in your name. If you have trouble with falsified accounts, contact the Public Utility Commission.

You are not responsible for losses from ID theft.

Your credit should not be permanently affected.

Do not be coerced into paying a fraudulent debt.

Your Rights

Under Federal Laws/Rules, You Have the Right to:

- Request a free copy of your credit report once a year from each of the three credit reporting agencies. If you dispute credit report information, credit bureaus must resolve your dispute within 30 days and send you written notice of the results of the investigation, including a copy of the credit report, if it has changed.
- 'Opt Out' of credit card companies and banks' marketing programs, including 'convenience checks' sent on your credit card account by calling the companies' customer service numbers.
- "Opt Out" of credit card solicitations:1-888-567-8688, www.optoutprescreen.com
- Report unauthorized checking transactions within 30 days of receiving your bank statement with $50 liability protection.
- Report unauthorized credit card transactions within 60 days of receiving your statement with $50 liability protection.
- Report electronic funds transfer/online banking problems within two days with $50 liability protection; report within 60 days for a $500 liability cap.

Under Colorado law, you have the right to:

- Request a courtesy law enforcement report in the community in which you live or in the community where you know the theft occurred.
- Send a copy of your law enforcement report or Federal Trade Commission affidavit to credit reporting agencies to protect your credit.
- Remove your SSN from driver's licenses and health insurance cards.
- Have only the last four digits printed on your credit card receipts.
- Have your identity verified by credit card solicitors before they send a credit card to an address different from yours.
- Have the right to ask businesses, non-profit, government agencies about their policies for disposal of personal identifying documents.
- Freeze your credit report (See next page.)

MUST I PROVIDE MY SOCIAL SECURITY NUMBER TO BUSINESS?

Reprinted from the Social Security Administration Website, www.ssa.gov

The Social Security Number (SSN) was originally devised to keep an accurate record of each individual's earnings, and to subsequently monitor benefits paid under the Social Security program. However, use of the SSN as a general identifier has grown to the point where it is the most commonly used and convenient identifier for all types of record-keeping systems in the United States. Specific laws require a person to provide his/her SSN for certain purposes. While we cannot give you a comprehensive list of all situations where an SSN might be required or requested, an SSN is required/requested by:

- Internal Revenue Service for tax returns and federal loans.
- Employers for wage and tax reporting purposes.
- States for the school lunch program.
- Banks for monetary transactions.
- Veterans Administration as a hospital admission number.
- Department of Labor for workers' compensation.
- Department of Education for Student Loans.
- States to administer any tax, general public assistance, motor vehicle or driver's license law within its jurisdiction.
- States for child support enforcement, and for support to needy families.
- States for commercial driver's licenses.
- States for Food Stamps, Medicaid, and Unemployment Compensation.
- U.S. Treasury for U.S. Savings Bonds.

The Privacy Act regulates the use of SSN's by government agencies. When a Federal, State, or local government agency asks an individual to disclose his or her Social Security number, the Privacy Act requires the agency to inform the person of the following:

- the statutory or other authority for requesting the information;
- whether disclosure is mandatory or voluntary;
- what uses will be made of the information;
- the consequences, if any, for failure to provide the information.

If a business or other enterprise asks you for your SSN, you can refuse to give it. However, that may mean doing without the purchase or service for which your number was requested.

For example, utility companies and other services ask for a Social Security Number, but do not need it; they can do a credit check or identify the person in their records by alternative means. Giving your number is voluntary, even when asked for the number directly.

If requested, you should ask why your number is needed, how your number will be used, what law requires you to give your number and what the consequences are if you refuse. The answers to these questions can help you decide if you want to give your Social Security Number.

The decision is yours.

For more detailed information, we recommend the publication at:
http://www. socialsecurity.gov/pubs/10002.html.

CREDIT SECURITY FREEZE

A freeze means your file cannot be shared with potential creditors. If your credit files are frozen, even someone who has your name and Social Security number will not be able to get credit in your name.

How do I place a security freeze?
Instructions for residents of each state are slightly different. Fortunately, the three credit bureaus have simple grids on their Web sites explaining what the costs are and the process is. Remember, you have to get a freeze at all three bureaus.

Equifax

General info: *http://www.equifax.com/securityfreeze/index.html*

State-by-state information

http://www.equifax.com/securityfreeze/state_file_freeze_grid.html

To get a freeze, Equifax send a certified letter with seven specific elements to Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348. The elements are spelled out clearly on the general information page, but they are, basically -- name, address, date of birth, SSN, utility bill for proof of address, payment and a police report if you are a victim.

Experian

General info and state-by state information

http://www.experian.com/consumer/security_freeze.html

To get state-specific information, scroll to the bottom of the page and pick your state from the drop-down menu. Before giving you the information you need, Experian will warn you that a security freeze may make your credit life very difficult. Take that with a grain of salt, and then pick your state. You'll send the request by certified or overnight mail to Experian, P.O. Box 9554, Allen, TX 75013. Again, the recipe is listed on the firm's Web site, but it will call for a name, SSN, date of birth, current and past addresses dating back two years, a copy of your driver's license, and one utility bill.

TransUnion

General info and state-by-state information

http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page

Send your freeze requests to Trans Union/Fraud Victim Assistance Department, P.O. Box 6790, Fullerton, CA 92834. A few state residents can call instead of write -- check

the link above. Trans Union wants the following on the letter: name, address, Social Security Number, a copy of your driver's license and payment.

You must include:
☐ Full name, with middle initial and generation, such as Jr., Sr., III;
☐ 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).

Do I have to freeze my file with all three credit bureaus?
Yes. Different credit issuers may use different credit bureaus.

Can I open new credit accounts if my files are frozen?
Yes, if you want to open a new credit account, you can lift the freeze for a specific creditor or period of time. When you freeze your files, you will receive a unique PIN from each of the agencies as well as how to lift the freeze. You can lift the freeze by phone using your PIN and proper identification.

Is there a fee to freeze my credit files?
The initial security freeze is free of charge; however, the temporary or permanent removal of the freeze may cost up to $10 per agency.

How long does it take the freeze to be in effect and how long does it take for a freeze to be lifted?
Credit bureaus must place the freeze no later than five business days after receiving your written request. A freeze must be lifted no later than three business days after receiving your request.

What will a creditor who requests my file see if it is frozen? Can someone get my credit score?
A creditor will see a message or a code indicating that the file is frozen and will not be able to get your credit score.

Can I order my free credit report if the file is frozen?
Yes, free credit reports from each credit bureau are available every 12 months at www.annualcreditreport.com or 1-877-322-8228.

Can anyone see my credit file if it is frozen?
Yes, certain entities will have access to it. Your report may be released to existing creditors or to collection agencies acting on their behalf. They can use it to review or collect on your account. Other creditors may use your information to make offers of credit unless you opt out of such offers (see below) Government agencies may have access for child support payments or taxes, for investigating Medicare/Medicaid fraud, or in response to a court/administrative order, subpoena, or search warrant delinquent taxes or unpaid court orders.

Does freezing stop pre-approved credit offers?
No. To stop pre-approved credit solicitations, you need to "opt out" at www.optoutprescreen or call 1-888-567-8688. It's good for five years or you can make it permanent. You will need to key in your Social Security number.

Can an employer do a background check on me if I have a freeze on my credit file?
No. You would have to lift the freeze to allow a background check just as you would to apply for credit.

What is the difference between a fraud alert and a freeze?
A fraud alert on a report tells a potential credit issuer that there may be fraud. A fraud alert can help prevent identity theft and can also slow your ability to get new credit. A freeze means your credit file cannot be seen by potential creditors or employers doing background checks unless you give your consent.

RESOURCES

Credit Card Offer "Opt Out" Line

To stop credit card offers or unwanted credit cards. This is a free call and a free service. You will be asked to give your Social Security Number.

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

Credit Reporting Agencies

To request a FREE copy of your Credit Report from all three CRAs (you need your Social Security Number and other verifying information.)

Website: www.annualcreditreport.com
(Do not use www.freecreditreport.com)
Phone: 877-322-8228

Or download a copy of the Annual Credit Request Form at:

www.annualcreditreport.com and mail it to:
Annual Credit Report Request Service
P.O. Box 105281, Atlanta, GA 30348-5281

To report theft or unauthorized use of your credit card or SSN, contact:

Equifax 1-800-525-6285, www.equifax.com
Experian 1-888-397-3742, www.experian.com
Trans Union 1-800-680-7289, www.transunion.com

ID Theft Assistance

- **Federal Trade Commission - www.consumer.gov/idtheft**
  1-877-ID-Theft
- **Colorado Attorney General - www.ago.state.co.us/idtheft**
- **Identity Theft Resource Center – www.idtheftcenter.org**

Social Security Administration

For your **Earnings & Benefit Estimate Statement** call: **1-800-772-1213**
Or request the form online at **www.ssa.gov/mystatement**
or download the form at **www.ssa.gov/online/ssa-7004.html**

INTERNAL REVENUE CONTACTS

- To verify that the IRS actually sent a notice, call 1-800-829-1040
- To report an IRS related fraud, call the tax-fraud referral hot line 1-800-366-4484
- If identity theft has caused problems with the IRS, call: IRS Identity Protection Specialized Unit 800-908-4490
- If you have a problem with the IRS that you cannot resolve, call: Taxpayer Advocate for Colorado 303-446-1012

INTERNET SCAMS

To report an Internet-based scam, go to https://www.ic3.gov/crimeschemes.aspx

OPT OUT OF COMMERCIAL E-MAIL AND DIRECT MAIL

($1.00 fee) To eliminate much of the junk mail filling your mailbox, contact the Mail Preference Service and send the following letter:

Mail Preference Service
PO Box 643 Carmel, NY 10512

To Whom It Concern:

Please remove my name from your marketing lists. Thank you for your attention to this matter.

My name and address are:

Your name Your mailing address City, State, Zip Code

Or you can go to their website and register on-line at: www.dmaconsumers.org

PASSPORT ISSUES

If your passport is stolen or being used fraudulently: **www.travel.state.gov/passport_services.html** or call a local U.S. Department of State field office.

Report Fraud

For questions relating to fraud and fraud prevention, call:

- **Denver District Attorney Economic Crime Specialists**
  Hotline: 720-913-9179

- Arapahoe, Douglas, Lincoln and Elbert Counties'
  District Attorney Assistance Line: 720-874-8547
- Boulder County District Attorney 303-441-3789
- Jefferson and Gilpin Counties' District Attorney 303-271-6980

Amc@denverda.org with "subscribe" in the subject line.

To schedule a *Stand Up Against Fraud presentation*, contact:
To sign up for Denver DA Monthly Fraud Newsletter send an email to:

Maro Casparian
2nd Judicial District
Denver DA's Office
720-913-9036, amc@denverda.org