



As District Attorney, I am concerned with the rise of identity theft in our community. Many of us unknowingly subject ourselves to the potential theft of valuable information that can be used to destroy our credit, wipe out savings accounts, and otherwise subject us to an unwanted invasion of our privacy.

There are many steps that we can take to minimize our exposure to the criminal acts that can affect us so severely. In an effort to inform you of these steps, I have compiled information for this booklet from District Attorneys, law enforcement agencies as well as various articles and publications.

However, information alone is not enough; we must actively involve ourselves in changing habits that put us at risk.

Hopefully, this booklet will help you become more knowledgeable, and as a result, provide you with tools and personal practices that may help protect you from identity theft.

A handwritten signature in cursive script that reads "Larry R. Abrahamson". The signature is written in black ink and is positioned above the printed name.

Larry R. Abrahamson
District Attorney

TABLE OF CONTENTS

ACCORDING TO THE ATTORNEY GENERAL	1
WHAT IS YOUR IDENTITY THEFT PROBABILITY (ITP) SCORE	3
MINIMIZE YOUR RISK OF ID THEFT	5
IF YOUR IDENTITY IS STOLEN	8
YOUR CONSUMER AND VICTIM RIGHTS	9
PROTECT YOUR SOCIAL SECURITY NUMBER	11
IDENTITY AFTER DEATH	13
RESOURCES	14

A RESOURCE GUIDE FOR IDENTITY THEFT PREVENTION AND VICTIM ASSISTANCE

Be Cautious - Know Your Rights - Stay Safe

ACCORDING TO THE COLORADO ATTORNEY GENERAL



Identity theft refers to the unauthorized use of personal identifying and financial information for the purpose of stealing your money and your good credit. Identity thieves look for driver's license information; social security numbers; bank account, credit card and calling card numbers; and information on a potential victim's investment accounts. They may review a person's spending habits and even family information (maiden names, children's names or other "personal" information used by many people as passwords on protected accounts). Identity thieves will use that information to empty out existing bank accounts, run up huge charges on your credit cards, and even apply for new credit cards and loans in your name.

A nationwide survey released by the Federal Trade Commission in September 2003 found that identity theft is an even bigger problem than originally believed. According to that survey, more than 9.9 million Americans were the victims of identity theft last year alone, losing a collective \$5 billion. Businesses, including financial institutions, lost more than \$50 billion due to identity theft. A copy of the complete FTC survey report is available at: www.ftc.gov/os/2003/09/synovatoreport.pdf.

According to the FTC database for 2002, complaints by Colorado victims of identity theft involved the following types of fraud:

Credit card fraud	35%
Bank fraud	21%
Phone or utilities fraud	19%
Employment-related fraud	13%
Government documents/benefits fraud	8%
Loan fraud	6%
Other	19%
Attempted identity theft	7%

For many victims, identity theft is about more than the loss of money. It is about the loss of security, independence and self-worth. A person may be consumed with: endless paperwork, pleading with creditors, and fending off debt collectors. They never know when or if it will stop.

WHAT IS YOUR IDENTIFY THEFT PROBABILITY (ITP) 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. I have new boxes of checks mailed to my home. **10 points** _____
4. I have not “opted out” of my credit card marketing programs and receive “convenience” checks on my account in the mail. **10 points** _____
5. I carry a purse or wear my 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 **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.

MINIMIZE YOUR RISK OF ID THEFT

Be Proactive, Don't Wait Until You Are a victim



After scoring your ITP - it is now time to do the following:

- Mail bills at your post office, not in your mailbox or corner mail drop. Consider using automated payment plans.
- 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’ check mailings.
- Carry sensitive information in a close fitting pouch or in your front pocket, not in your purse or wallet – this includes: 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.
- Copy credit cards or any identification information that you carry in 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 (it’s free and there is no limit to how often you may request it) 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 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.
- Keep your financial and tax records in locked files in your home or office.
- Don't 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. Seldom does anyone other than an employer, the I.R.S., or the Colorado Department of Motor Vehicle need your Social Security Number.
- 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. Use a crosscut shredder.
- Don't respond to e-mails asking to submit personal data. The message might include fancy graphics, trademark symbols and an authentic-looking e-mail address, but all of that can be faked. Here are some ways to tell:
 - ✓ The message tries to scare you saying your account needs to be verified or updated.
 - ✓ The message threatens negative action – for example: canceling your account if you fail to take the requested action immediately.
 - ✓ The message asks you to click on a link to update your information 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.
- Install a firewall program if you use a high-speed connection cable, DSL or T-1, which connects your computer 24 hours a day. A firewall stops uninvited guests from accessing your computer. Without, hackers can access personal information on your computer 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.
- Don't let online merchants store your credit card number. Numerous data bases have been hacked into by identify thieves.
- Use a different password for each account and keep your records of the accounts in a safe place - not on your computer.

Perpetrators have many ways of gaining access to personal information. Following is a list of methods commonly used to access the information for identity theft*:

- Stealing wallets and purses that contain identification, credit cards, and bank cards - a common venue is the church pew.
- Stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, and tax information.
- Completing a "change of address form" to divert mail to a different location.
- Rummaging through trash for personal data (commonly called "dumpster diving").
- Fraudulently obtaining credit reports by posing as a landlord, mortgage broker, employer, or other party who may have a legitimate need and the legal right to access the information.
- Absconding with personal information found in a private residence—invitees and family might be the ones abusing the trust of an elder.
- Simply asking for it: "phishing" is a manner of posing as a legitimate bank or business, contacting customers, and asking them to use a link in an e-mail message to update or verify their personal information.
- Acquiring information from employers or businesses, using a practice known as "business record theft," which involves stealing files from offices where the victim is an employee, customer, patient, or student (perpetrators may bribe an employee who has access to client files or "hack" into electronic files).

****(Printed with permission: 40 The Colorado Lawyer 46, (Oct., 2005) - Protecting Clients From Abuse and Identity Theft - Paul O. Mitchell and D. Wayne Stewart)***

IF YOUR IDENTITY IS STOLEN

Resolving the consequences of identity theft is left largely to the victims. Act quickly and assertively, and keep records/copies of all contacts and reports. The Colorado Attorney General's website has a step-by-step guide for victims of identity theft, which includes:

- File a report with your police/sheriff and get a copy of the report for the credit agencies, banks and credit card companies. You may also download and complete the Federal Trade Commission Affidavit.
- 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 don't need this! Carefully monitor your credit card statements for evidence of fraudulent activity.
- Contact your financial institution and cancel all accounts and PIN numbers. Stop payments on outstanding checks and complete an "affidavit of forgery" on unauthorized checks. Your bank or financial institution can provide you with the "affidavit of forgery" for you to complete.
- Report the theft to one of the credit reporting agencies fraud units (note credit agencies on Page 14). The agency will notify the other two of the possible fraud. Request the credit reporting agencies to flag your credit file for fraud. Add a victim's statement to your report, such as: **"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 - therefore:

- Your credit should not be permanently affected.**
- No legal action should be taken against you.**
- Cooperate, but don't be coerced into paying a fraudulent debt.**

YOUR CONSUMER & VICTIM RIGHTS



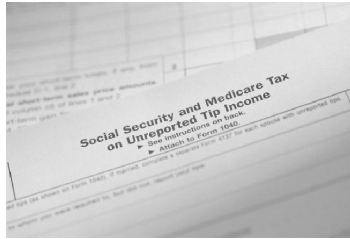
Under Federal Law, You Have the Right to:

- 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 at 1-888-567-8688 or www.optoutprescreen.com.
- Report unauthorized checking transactions within 30 days of receiving your bank statement – normally there will be a \$50 liability protection.
- Report unauthorized credit card transactions within 60 days of receiving your statement - \$50 liability protection.
- Report electronic funds transfer/online banking problems within two days - \$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 the credit reporting agencies to protect your credit file.
- Have your SSN removed from a driver's license/ID card, and health insurance card.
- Have only the last four digits of your credit card printed on credit card receipts.
- Request that credit card solicitors obtain identity verification before they send a credit card to an address different than yours.
- Have the right to ask businesses, non-profit, government agencies about their policies for disposal of personal identifying documents.

PROTECT YOUR SOCIAL SECURITY NUMBER



Treat your Social Security number (SSN) as confidential information and avoid giving it out unnecessarily. Keep your Social Security card in a safe place with your other important papers. Do not carry it with you unless you need to show it to an employer or service provider.

Merchants and businesses can request your Social Security Number, but you do not have to provide it to them.

The Social Security Administration (SSA) protects your SSN from misuse. They require and carefully inspect proof of identity from people who apply to replace lost or stolen Social Security cards or corrected cards. The SSA maintains the privacy of Social Security records unless:

- **The law requires the disclosure of information to another government agency; or**
- **Your information is needed to conduct Social Security or other government health or welfare program business.**

HOWEVER, your Social Security Number is not required to do a credit check.

Be very careful about sharing your number and card to protect against misuse of your number. Giving your number is voluntary even when you are asked for the number directly. If requested, you should ask:

- **Why your number is needed;**
- **How your number will be used;**
- **What happens if you refuse; and**
- **What law requires you to give your number?**

The answers to these questions can help you decide if you want to disclose your Social Security number. The decision is yours.

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

Be proactive - don't wait until it happens to you.

Consumer Report states:

Five ways to outwit identity theft thieves

1. Never directly respond to email asking for personal information.
2. If you doubt a message's authenticity, verify it by contacting the institution itself.
3. Avoid spoofed sites by entering web addresses directly into the browser yourself or by using bookmarks you create.
4. When prompted for a password, give an incorrect one first. A phishing site will accept it - a legitimate one won't.
5. A secure web site gives you more assurance. To see whether a site is secure, look at the bottom of your browser's window for a icon of an unbroken key or a lock that's closed, golden, or glowing. Double-click on the lock to display the site's certificate, and make sure it matches the company you think you're connected to.

Forward the fraudulent spam to the Federal Trade Commission at spam@uce.gov and Anti-Phishing Working Group at reportphishing@antiphishing.org

A good reference book is: Johnny Mays guide - **[How To Prevent Identity Theft.](#)**

IDENTITY THEFT AFTER DEATH



Very little is required to steal the identity of a deceased person; all that is necessary is a name, Social Security number, and the information on the death certificate. With this information, a thief can complete a credit card application and request that the new card be sent to an address of the thief's choosing. The thief can make purchases and, after a few weeks, move on to the next victim before the surviving family members become aware that a fraud has been perpetrated. Although a surviving spouse is not likely to be liable for such purchases, his or her credit could be negatively affected by unauthorized transactions in the deceased spouse's name.

RESOURCES



1. **Credit Card Offer “Opt Out” Line**

Used to stop credit card offers or unwanted credit cards, this is a credit reporting industry free call and a free service. You will be asked to give your Social Security Number. 1-888-567-8688

2. **Credit Reporting Agencies**

Website: www.annualcreditreport.com

(Do not use: www.freecreditreport.com - there will be a charge)

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 fraud on your credit card or get a credit report contact:

Equifax

www.equifax.com

To report fraud call: 1-800-525-6285,

To order report call: 1-800-685-1111

Experian www.experian.com
To report fraud call:
1-888-397-3742 or 1-800-972-0233
To order report call: 1-888-397-3742

Trans Union www.transunion.com
To report fraud call:
1-800-680-7289 or 1-877-553-7803
To order report call: 1-800-888-4213

To request a FREE copy of your Credit Report from any of the three CRAs, you need your Social Security Number and other verifying information.

3. ID Theft Assistance

For a copy of the Federal Trade Commission ID Theft Affidavit:
www.consumer.gov/idtheft or 1-877-ID-Theft

Identity Theft Resource Center – Sample victim letters:
www.idtheftcenter.org

4. Social Security Administration

For your Earnings & Benefit Estimate Statement (Form SSA-7004)
Phone: 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

5. General State Information

Colorado Attorney General web site: www.ago.state.co.us/idtheft/IDTheft.cfm

Colorado Department of Motor Vehicles: www.revenue.state.co.us/mv_dir/wrap.asp?incl+mvinvwebpage

6. General Federal Information

National Fraud Center: www.fraud.org

NOTES
