

*POWER AGAINST
IDENTITY THEFT
HANDBOOK*

Denver District Attorney

Mitch Morrissey



CASE is a Partnership of the District Attorney and
the Community to Prevent Fraud and Exploitation

Fraud Assistance Line

720-913-9196 or 720-913-9179

www.denverda.org

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.

REDUCE YOUR ID THEFT RISK

- Mail bills to be paid at the Post Office, not in your mailbox or in street corner postal boxes. 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’ 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.)
- Don’t 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.
- 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.
- 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.
- Don't 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.

IF YOUR IDENTITY'S STOLEN

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

- File a report with your police/sheriff and get a copy of the report for the credit agencies, banks and credit card companies. Or request and complete the ID Theft Affidavit from the Federal Trade Commission.
- 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 "affidavits of forgery" on unauthorized checks.
- Report the theft to one of the fraud units of the credit reporting agencies. That 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.
Your credit should not be permanently affected.
No legal action should be taken. Cooperate, but don't 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 than yours.
- ◆ Have the right to ask businesses, non-profit, government agencies about their policies for disposal of personal identifying documents.
- ◆ Freeze your credit report (effective July 1, 2006.)

RESOURCES

1. 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

2. 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

3. 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

4. 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