The fastest growing white-collar crime in the US.

IDENTITY THEFT REPAIR KIT

BROUGHT TO YOU BY:

COLORADO ATTORNEY GENERAL

JOHN SUTHERS

KNOW HOW TO
PROTECT YOURSELF

Message from Attorney General John Suthers

Dear Coloradans:

Identity theft is the fastest growing crime in America. Each year, millions are victimized by this senseless crime. Technological advances and the proliferation of the Internet have only enhanced our exposure to thieves seeking to steal our identities.

Identity theft may come in multiple forms, but its impact is always frustrating and oftentimes devastating. In fact, anyone can be a victim of identity theft. For this reason, it is vital that Coloradans understand how to protect themselves.

Please use this handbook to help you avoid becoming a victim of identity theft, and guide you through the important steps of repairing the damage done in case you do fall victim.

I hope that you will find this guide a helpful resource.

John W. Suthers

Table of Contents

INTRODUCTION 1

What is Identity Theft? 2
How do thieves get my personal or financial information? 3
What do they do with it? 4
Identifying Identity Theft 4

10 STEPS TO TAKE IF YOU BECOME A VICTIM 7

Step 1: Contact your bank and other credit card issuers 7
Step 2: File a report with your local law enforcement agency 7
Step 3: File a report with the FTC 8
Step 4: Contact all three major credit reporting bureaus 8
Step 5: Contact all of your creditors by phone and in writing 11
Step 6: Notify the phone company 11
Step 7: Notify the post office 11
Step 8: Notify the Social Security Administration 12
Step 9: Notify the State Department 12
Step 10: If you are contacted by a collection agency 12

LIABILITY 15
Security Freeze 15

CHECKLISTS 16
Plan of Action List
Document List

TIPS ON PREVENTING ID THEFT 18

CONTACTS 20

The information contained within this booklet is for educational purposes only and should not be substituted for the advice of an attorney licensed to practice law in Colorado.

1st publication 2007

YOU ARE A VICTIM of IDENTITY THEFT

Someone has obtained access to your checking account, stolen your debit card, or ruined YOUR CREDIT HISTORY

credit denied

WHAT Happened?

You've just come home from a long day at work. The mail is here. More bills. It's just what you need after all the stress from a presentation that is already past deadline. You open your debit card statement. You didn't buy much this month—just some groceries and some clothes. Halfway up the driveway you stop. The statement shows an overdraft. You had more than $1,000 in your checking account the last time you took out money and now you are more than $50 in the negative.

You've finally saved up for a car. You've been waiting to get your very own car ever since you graduated from college. You've just picked out a beautiful little blue sports car and the salesman is off putting together the paperwork. Just as you are admiring what will soon be your new ride, the salesman comes up with a sad look on his face. "It's your credit," he says. "I'm sorry."

The police knock on your door. They have a search warrant. They inform you that your name, address, and phone number have been connected to a website containing child pornography. But you've never built a website and you only use your computer for balancing your checkbook and checking your email.

What happened?

You are a victim of identity theft. Someone has obtained access to your checking account or stolen your debit card. Someone has ruined your credit history by opening credit accounts in your name that haven't been paid off. Someone has gotten hold of your credit card number, either by stealing it, hijacking your computer, or by any number of other ways. Someone has used your personal information to conduct illegal activities. Now that your credit history is ruined and you are in debt for things you never knew about, you can't qualify for an auto loan to buy a car or pay for those perfect shoes. You could be in danger of being arrested for something you didn't do.

Now what?

WHAT IS IDENTITY theft?

Identity theft occurs when someone fraudulently uses your personal identifying information to obtain credit, take out a loan, open accounts, get identification, or any other activity in which a criminal uses your information in an unauthorized way.

Estimates from the Federal Trade Commission suggest that identity theft is on the rise. In fact, identity theft is the fastest growing crime in the country—a crime that affects Coloradans and their credit histories.

According to the FTC database for 2009, complaints by Colorado victims of identity theft involved the following types of fraud:

Credit card fraud	15%
Bank fraud	8%
Phone or utilities fraud	13%
Employment-related fraud	25%
Government documents or benefits fraud	14%
Loan fraud	3%
Other	23%
Attempted identity theft	5%

How Do Thieves Get My Personal or Financial Information?

Here are some of the ways identity thieves steal your personal and financial information:

- **Stealing your purse or wallet** to obtain social security cards, credit cards, driver's licenses, etc.
- **Stealing mail** being delivered to your home or left out for pick-up.
- **Diverting your mail** to another mailbox using a false "change-of-address" request.
- **"Dumpster diving"** – thieves dig through dumpsters or garbage cans behind homes or businesses looking for discarded checks or bank statements, credit card or other account bills, medical records, pre-approved credit applications, etc.
- **"Shoulder surfing"** – thieves watch over your shoulder as you enter your PIN into an ATM or as you key your long-distance calling card number into a pay telephone.
- **"Pretext calls"** – thieves call to "verify" account information or to "confirm" an enrollment or subscription by having you repeat bank or credit card account numbers.
- **Using false or misleading Internet sites** to collect personal and financial information.
- **Purchasing personal information** from unscrupulous employees at companies with which you do business.
- **Burglarizing homes** looking for purses, wallets, files containing personal and financial information.
- **Burglarizing businesses** looking for computers or files containing personal and financial information on clients.
- **Computer hackers** "breaking into" business or personal computers to steal private client files and personal financial information.
- **Phony e-mail or "pop-up" messages** that appear to be from your credit card company, Internet Service Provider or other entity you do business with. These phony messages claim some problem with your account and direct you to another web site where you will be asked to supply credit card and other personal information.
- **ATM skimming** involves the placement of a mechanical card reader over or into the actual card reader on an ATM machine. These fake card readers will capture your account number and possibly even your PIN code, which are then used to produce counterfeit credit or debit cards.

What do they do with it?

- **Drain your bank account** with electronic transfers, counterfeit checks, or your debit card.
- **Open a bank account in your name** and write bad checks with it.
- **Open a credit card account** that never gets paid off, which gets reflected on your credit report.
- **Use your name if they get arrested** so it goes on your record.
- **Use your name for purchases involved in illegal activities**, such as products for methamphetamine production or an Internet domain for a child pornography site.
- **Use your name to file for bankruptcy or avoid debts**.
- **Obtain a driver's license** with your personal information.
- **Buy a car** and use your information and credit history to get a loan for it.
- **Obtain services in your name**, such as phone or Internet.

Identifying Identity Theft

Here are some warning signs that you may be the victim of identity theft:

- You are denied credit.
- You find charges on your credit card that you don't remember making.
- Personal information, credit cards, ATM cards, checks, or IDs have been stolen from you.
- You suspect someone has fraudulently changed your mailing address.
- Your credit card bills stop coming.
- You find something wrong with your credit report, such as loans you didn't take out or accounts you don't remember opening.
- A debt collector calls about a debt you don't owe and didn't know about.

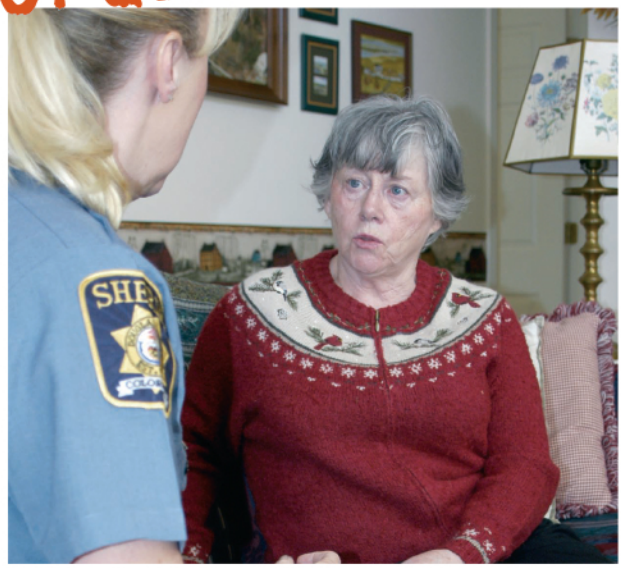
You could be the victim of identity theft without noticing any of these things happening to you, so it is always a good idea to keep a careful eye out for anything out of the ordinary by ordering your credit report at least once a year and being alert to these warning signs.

ORDER YOUR CREDIT REPORT

at least once a year

A free credit report is available at www.annualcreditreport.com.

ACT QUICKLY



File a police report.

10 Steps to take if you become a victim

If you believe that you are a victim of identity theft, there are a number of important steps for you to follow. Be prepared to document all unauthorized transactions and to be patient as the process can take a number of months.

Step 1: CONTACT YOUR BANK AND OTHER CREDIT CARD ISSUERS

If the theft involved existing bank accounts (checking or savings accounts as well as credit or debit cards) you should take the following steps:

- Put stop payment orders on all outstanding checks that might have been written without your knowledge or permission.
- Close all existing credit card accounts and any account accessible by debit card.
- Open up new accounts protected with a secret password or personal identification number ("PIN").

  DO NOT use the same passwords or PINs as on the original accounts.
- Do not use common numbers (like birth dates, part of your social security number), or commonly chosen words (such as a child's, spouse's, or pet's name) as passwords or PINs.

Step 2: FILE A REPORT WITH YOUR LOCAL LAW ENFORCEMENT AGENCY

Obtaining that report will help you in dealing with your banks, creditors, and the major credit reporting bureaus (see Step 4).

CRIMINAL VIOLATIONS:
If an identity thief has impersonated you when they were arrested or cited for a crime, there are things you can do to correct your record. First of all, to prevent being wrongfully arrested, carry copies of documents showing that you are a victim of identity theft even if you do not know that criminal violations have been attributed to your name. If they have, contact the law enforcement agency (police or sheriff's department) that arrested the identity thief. Or if there is a warrant for arrest out for the impersonator, contact the court agency that issued it. You may also want to get a lawyer to help you.

Step 3: FILE A REPORT WITH THE FEDERAL TRADE COMMISSION

The Federal Trade Commission maintains an Identity Theft Data Clearinghouse. The FTC aids identity theft investigations by collecting complaints from identity theft victims and sharing the information with law enforcement agencies, credit bureaus, companies where the fraud took place, and other government agencies.

File a complaint with the FTC by going to www.consumer.gov/idtheft or by calling their toll-free number: 1-877-ID-THEFT (1-877-438-4338). Many creditors and the major credit reporting bureaus will accept the "ID Theft Affidavit" available on this FTC web site.

IDENTITY THEFT AFFIDAVIT: Fill out the Identity Theft Affidavit offered by the FTC. This form will help you report information about your identity theft with just one form. Many companies accept this form, though others will require you to use their own form or submit more forms. If a new account has been opened in your name, you can use this form to provide the information that will help companies investigate the fraud. Once you have filled out the ID Theft Affidavit as completely and accurately as possible, mail a copy to any of the companies concerned with the fraud, such as banks or creditors. More information on the ID Theft Affidavit can be found at www.consumer.gov/idtheft. Make sure that you keep copies of all of your paperwork, including records of everyone you have corresponded with, fraudulent bills, police reports, and complaint forms.

Step 4: CONTACT ALL THREE MAJOR CREDIT REPORTING BUREAUS

First, ask the credit bureaus to place a "fraud alert" on your file. You must then be contacted directly before any new credit is taken out in your name. Second, file your police report (Step 2), immediately with the credit reporting bureaus. Colorado law requires the credit bureau to then block any new, negative credit information resulting from the theft of your identity. A fraud report filed with one bureau will be shared with the other bureaus.

CREDIT BUREAUS

EQUIFAX
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241
1-888-766-0008

EXPERIAN
www.experian.com
P.O. Box 9532
Allen, TX 75013
1-888-EXPERIAN (397-3742)

TRANSUNION
www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289

Contact all three credit bureaus IMMEDIATELY.

FILE

FRAUD ALERT

Keep copies of all correspondence to creditors.

Step 5: CONTACT ALL OF YOUR CREDITORS BY PHONE AND IN WRITING

File a law enforcement report, or the FTC's ID Theft Affidavit, with each creditor (some may require that you use their own form of affidavit).

- Keep copies of all correspondence and documents exchanged with each creditor.
- Cancel all existing credit card accounts and open replacement accounts. Ask that those cancelled accounts be processed as "account closed at customer's request" to avoid any negative reporting to credit bureaus.
- If replacement accounts or credit cards require passwords or PINs to access, **DO NOT** use the same passwords or PINs as on the original accounts.
- Do not use common numbers (like birth dates, part of your social security number), or commonly chosen words (such as a child's, spouse's, or pet's name) as passwords or PINs.

Step 6: NOTIFY THE PHONE COMPANY

If the identity theft involves the misuse of a long-distance telephone account, cellular telephone, or other telephone service, contact your telephone or wireless company and immediately close all existing accounts. If replacement accounts require passwords or PINs to access, **DO NOT** use the same passwords or PINs as on the original accounts. Do not use common numbers (like birth dates, part of your social security number), or commonly chosen words (such as a child's, spouse's, or pet's name) as passwords or PINs.

Step 7: NOTIFY THE POST OFFICE

If you suspect that your mail has been stolen or diverted with a false change-of-address request, contact your local postal inspector. You can obtain the address and telephone number of your local postal inspector by visiting the United States Postal Service web site at www.usps.com/ncsc/locators/find-is.html.

Step 8: NOTIFY THE SOCIAL SECURITY ADMINISTRATION

If you suspect that someone is using your social security number to obtain credit or employment, contact the Social Security Administration's fraud hotline at 1-800-269-0271 (TTY: 1-866-501-2101). To check the accuracy of your work history, order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) and check it for accuracy. You can obtain a PEBES application at your local Social Security office or you can download one from the Social Security Administration web site: www.ssa.gov/online/ssa-7004.pdf.

Step 9: NOTIFY THE STATE DEPARTMENT

If your passport has been stolen, notify the passport office in writing to be on guard for anyone ordering a new passport in your name.

Contact:
US Department of State
Passport Services
Consular Lost/Stolen Passport Section
1111 19th Street, N.W.
Suite 500
Washington, D.C. 20036

877-487-2778

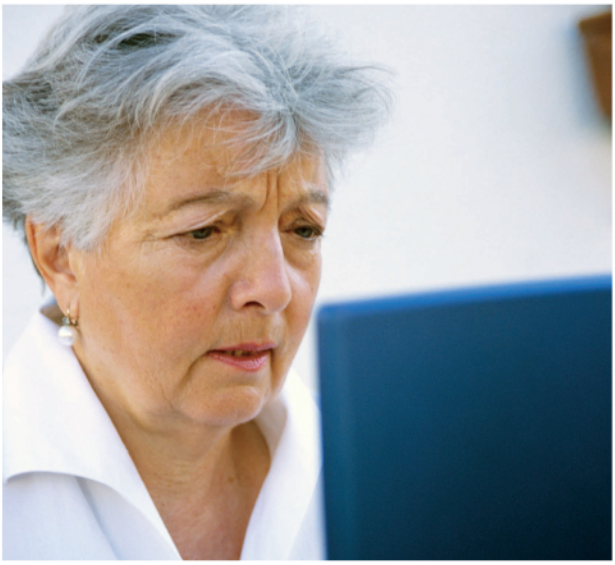
You can obtain additional information from their web site http://travel.state.gov/.

Step 10: IF YOU ARE CONTACTED BY A COLLECTION AGENCY

If you are contacted by a collection agency about a debt for which you are not responsible, immediately notify them that you did not create the debt and that you are a victim of identity theft. Follow up with the collection agency and creditor in writing and include a copy of your law enforcement report or ID Theft Affidavit. Send your letter, and copy of the report or affidavit, "return receipt requested," or with some other process that gives you proof that the collection agency received your letter. If the collection agency continues to contact you, file a complaint with the Colorado Collection Agency Board, 1525 Sherman Street, 7th Floor, Denver, CO 80203. 303-866-5304. Additional information is available on-line at www.coloradoattorneygeneral.gov/ca.

DO NOT GIVE UP

Clearing up the problems caused by identity theft can be time intensive, as well as an emotional and frustrating process. It can take weeks, and even months, of work contacting creditors and credit reporting bureaus. **DO NOT GIVE UP.** Exercise all of your consumer rights and retain an attorney if creditors and credit reporting bureaus are not cooperating with your efforts to clear your name and credit.



DON'T GIVE UP.

You can check your credit report online immediately at www.annualcreditreport.com.

Liability

To ensure that you don't end up paying hundreds or even thousands of dollars in fraudulent charges on your credit/debit cards made by an identity thief, the best course of action is to act quickly. The faster you act, the less liable you are for unauthorized charges.

CREDIT / DEBIT CARDS

According to the Truth in Lending Act, your liability is limited to $50 in unauthorized credit card charges per card in most cases. In order for this to come into effect, however, you must write to the creditor within 60 days of receiving the first bill that contained the fraudulent charge. If an identity thief changed your mailing address, you must still send your letter within 60 days of when you were supposed to have received it (**keep track of your bills!**).

If your ATM or debit card is lost or stolen, report it as quickly as possible. If you report it within two business days, you are only responsible for $50 in unauthorized withdrawals or transfers. If you report it between two and 60 days after, you may be responsible for up to $500 in unauthorized withdrawals or transfers the thief may make. If you do not report it after 60 days, you can lose any money the thief withdraws or transfers from your account after the 60 days.

report within 60 days

SECURITY FREEZE

In order to prevent unauthorized access to your credit reports, Colorado law allows you to place a "security freeze" on those reports. Contact each consumer reporting bureau (step 4 on page 8), **in writing by certified mail** and request that a freeze be placed on your account. You cannot be charged for the initial request. Once a freeze is in place, the bureau will not be able to release your credit report, or any information contained in the report, without your prior, express authorization. For more information about security freezes, including a list of those entities that will still be allowed to access your credit information, visit www.coloradoattorneygeneral.gov/idtheft.

Checklists

PLAN OF ACTION LIST

Because this is a lot of information to take in, we have provided you with a checklist to go through to make sure you have taken all the necessary steps after becoming an identity theft victim. Remember, you must complete all of these steps in a timely manner so that the identity theft does not get worse and to minimize your losses.

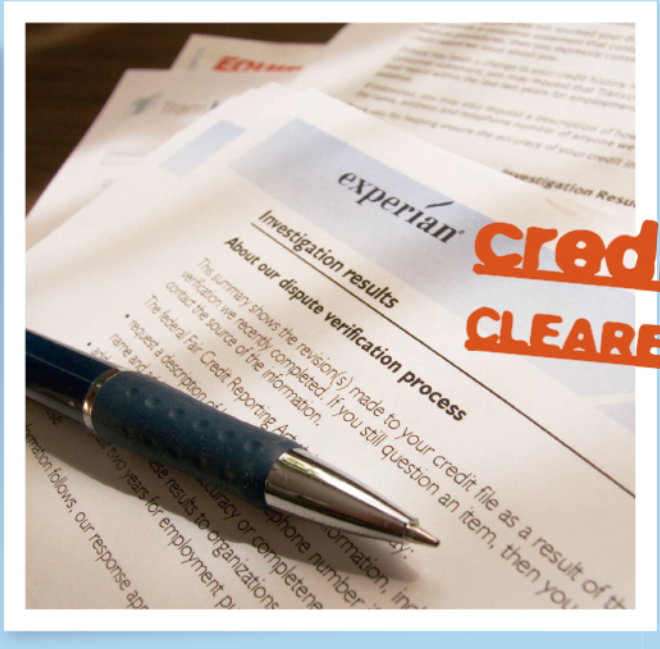
- ☐ 1. Filed a police report.
- ☐ 2. Obtained a copy of your credit report.
- ☐ 3. Identified errors, inquiries you did not know about, accounts you did not open, debts you did not know about, or anything else that seems wrong or out of place on your credit report.
- ☐ 4. Placed a fraud alert on your credit report.
- ☐ 5. Closed any accounts that might have been tampered with or opened without your knowledge or consent.
- ☐ 6. Contacted a major credit bureau by phone and by writing to correct inaccurate information.
- ☐ 7. Filled out the Identity Theft Affidavit.
- ☐ 8. Contacted the correct agencies to fix inaccurate information, close accounts, or report identity theft.
- ☐ 9. Filed a complaint with the Federal Trade Commission.

DOCUMENT LIST

Here is a list of documents you should have. You won't be able to keep the originals of some of the documents so it is very important that you make a copy for yourself.

It is also a good idea to keep copies of the documents that prove you are an identity theft victim with you, such as a copy of your police report.

- ☐ 1. Police report
- ☐ 2. Identity Theft Affidavit
- ☐ 3. Bills with fraudulent charges
- ☐ 4. Documentation of accounts opened in your name without your consent
- ☐ 5. Copies of letters sent to credit bureaus and creditors
- ☐ 6. Copies of all letters to and from collection agencies


experian
Investigation results
About our dispute verification process
Credit
CLEARED

Tips on preventing IDENTITY THEFT

There are a number of things you can do to minimize the chances that you will become a victim of identity theft:

- **NEVER** provide personal identifying or financial information during a telephone call you did not initiate. Banks, credit card companies, telephone companies and other legitimate creditors do not call to "verify" account numbers or to ask for your social security number or other personal information.

- **NEVER** provide personal identifying or financial information over the telephone to anyone claiming to represent a contest or sweepstakes promotion. It is illegal to market a foreign lottery in the United States. These calls are always fraudulent.

- **NEVER** carry your social security card in your purse or wallet.

- **NEVER** have your social security number printed on your checks, driver's license or other financial documents. If a bank, health care provider or other entity uses your social security number for client or account identification, call or write that company and ask that a different identification number be issued.

- **NEVER respond to e-mail or "pop-up" messages on your computer claiming some problem with a credit card, Internet, or other account.** Promptly contact your real credit card company or ISP to verify that there are no problems with your account.

- **Use a "cross-cut" shredder** and get in the habit of shredding all personal or financial documents before placing them in the trash. Shred copies of bills and invoices after you have paid them, bank statements (including your cancelled checks), investment or retirement account statements, pre-approved credit card or loan applications (especially those that come with a negotiable check attached), medical statements of any kind, and any other documents with information about you or your finances.

- **Password protect all credit card accounts that allow it.** Do not use common numbers or personal information (like birth dates or part of your social security number) or commonly chosen words (such as a child's, spouse's, or pet's name) for passwords.

- **Control access to your credit history.** Remove your name from mailing lists for pre-approved lines of credit by participating in the credit bureaus' "Opt-Out" program. Call 1-888-5-"OPT OUT" (1-888-567-8688) to enroll. You will need to provide your social security number to verify that you are making the request, but this is a legitimate use of such information.

- **Be careful with your incoming and outgoing mail.** If you don't have a secure, locked mailbox, mail your bills from a curbside public mailbox or directly at your local post office. **NEVER** leave outgoing mail in an unsecured mailbox overnight. If you are planning on being away from home, arrange with your post office to hold your mail.

- **Arrange to pick up new checks at your bank.** NEVER have boxes of new checks delivered to your home (they do not fit in many mail slots so your postal carrier may leave them on your doorstep).

- **Take all credit card or ATM receipts with you after you pay for goods or services.** Do not just leave them behind or throw them away in the trash can. Destroy them in your c ross-cut shredder when you get home.

- **Write to your bank, insurance company and other financial institutions you do business with and tell them not to share your customer information with unaffiliated third parties.** Under federal law, they are required to honor this request.

- **Remove your name from national direct mail advertising lists.** Contact the Direct Marketing Association at www.dmachoice.org.

- **To dramatically reduce telephone solicitations, sign up with the Colorado No-Call List.** Register on-line at www.coloradonocall.com or by calling 1-800-309-7041.

- **Participate in the national no-call registry** by going on-line at www.DONOTCALL.gov or by calling toll-free 1-888-382-1222 (TTY: 1-866-290-4236).

CONTACTS

Colorado Attorney General's Office

ID Theft: www.coloradoattorney general.gov/IDTheft

Ralph L. Carr Colorado Judical Center
1300 Broadway
Denver, CO 80203

(303) 866-4500
Consumer Line: 1-800-222-4444

Federal Trade Commission (FTC)

www.consumer.gov/idtheft

FTC
Identity Theft Clearing House
600 Pennsylvania Avenue N.W.
Washington, D.C., 20580
1-877-ID-THEFT
(1-877-438-4338)

Major Credit Bureaus

EQUIFAX: *www.equifax.com*
P.O. Box 740241
Atlanta, GA 30374-0241
1-888-766-0008

EXPERIAN: *www.experian.com*
P.O. Box 9532
Allen, TX 75013
1-888-EXPERIAN (397-3742)

TRANSUNION:
www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289

A free copy of your credit report is available from the website *www.annualcreditreport.com*

or write to:
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, Georgia 30348-5283

or call: 1-877-322-8228
TDD: 1-877-730-4104

Major Check Verification Companies

To find out if an identity thief has been passing bad checks in your name: SCAN 1-800-262-7771

To request a copy of your consumer report specifically about your checking account: Chex Systems, Inc. at 1-800-428-9623 or *www.chexhelp.com*

To request that your checks not be accepted by retailers:

Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120

TeleCheck at 1-800-710-9898 or 1-800-927-0188

Social Security Administration

www.ssa.gov

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
SSA Fraud Hotline: 1-800-269-0271

U.S. Postal Inspection Service

www.usps.gov/websites/depart/inspect

Call your local post office to find the nearest USPIS district office

Colorado Division of Motor Vehicles

Visit this website to find the DMV service center closest to you: *www.mv.state.co.us*

Colorado Bureau of Investigation – Identity Theft

690 Kipling Street
Denver, CO 80215
1-888-766-0008
Identity Theft Hotline:
1-855-443-3489

KNOW HOW TO
PROTECT YOU

COLORADO ATTORNEY GENERAL'S OFFICE | www.coloradoattorneygeneral.gov

Consumer Line **1.800.222.4444**

Colorado Attorney General's Office
Ralph L. Carr Colorado Judicial Center
1300 Broadway
Denver, CO 80203

WE ARE HERE TO HELP YOU!