Identity Theft Repair Kit

Brought to you by Colorado Attorney General Cynthia H. Coffman
Dear Coloradans,

Identity theft is one of the fastest growing crimes in America, impacting millions of households each year. The threat is more pervasive and the scams are more sophisticated than ever before. Identity thieves only need a few data points—like those found in widespread data breaches—and they can infiltrate your personal financial life, creating chaos. The damage can be life-altering.

Victims tell us that identity theft is about far more than the loss of money. It is about the loss of security and privacy. The destruction of hard-earned credit. The sense that someone who doesn’t even know you now can assume your identity.

Our goal at the Colorado Attorney General’s Office is to offer some useful tips to help you avoid becoming a victim of identity theft.

And because you can do everything right and still have your personal information stolen, we want to walk you through some important steps to take if you do become a victim.

With knowledge comes power. We want Colorado residents to feel empowered when it comes to protecting themselves from identity theft.

We hope you will find this guide a helpful resource.

Cynthia H. Coffman
# Table of Contents

**Introduction** .................................................................................. 5  
What is Identity Theft? ...................................................................... 6  
Emerging ID Theft trends ............................................................... 7  
How do thieves get my personal or financial information? ............. 9  
What do they do with it? ............................................................... 10  
Identifying Identity Theft .............................................................. 10  
Protecting your passwords .......................................................... 12  

**10 Steps to Take If You Become a Victim** .......................... 13  
Step 1: Contact your bank and other credit card issuers ............. 13  
Step 2: File a report with your local law enforcement agency ....... 13  
Step 3: File a report with the FTC ............................................. 13  
Step 4: Contact all three major credit reporting bureaus ............. 14  
Step 5: Contact all of your creditors by phone and in writing ..... 17  
Step 6: Notify the phone company ............................................ 17  
Step 7: Notify the post office ................................................... 17  
Step 8: Notify the Social Security Administration .................... 17  
Step 9: Notify the State Department .......................................... 18  
Step 10: If you are contacted by a collection agency .................. 18  

**Liability** .................................................................................. 20  
Credit/debit cards ........................................................................ 20  
Security freeze ............................................................................ 20  

**Checklists** ................................................................................ 21  
Plan of action list ........................................................................ 21  
Document list .............................................................................. 21  

**Tips on Preventing ID Theft** .................................................... 22  

**Contacts** .................................................................................. 24  

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.

Publication Date: August 2016
You Are a Victim of Identity Theft

Someone has obtained access to your checking account, stolen your debit card, filed taxes in your name, or ruined your credit history.
Credit Denied
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, Colorado victims filed more than 6,724 identity theft complaints in 2015 involving the following types of fraud:

- Government Documents or Benefits Fraud* 50%
- Credit Card Fraud 15%
- Phone or Utilities Fraud 6%
- Bank Fraud 6%
- Employment-Related Fraud 6%
- Attempted Identity Theft 3%
- Loan Fraud 2%

* Government Documents or Benefits Fraud includes the following subcategories of ID Theft: Tax- or Wage-Related Fraud, Government Benefits (Applied For/Received), Other Government Documents (Issued/Forged), and Driver's License (Issued/Forged).
Emerging ID Theft trends

**Income Taxes**

Income tax identity theft usually occurs in one of two ways:

- Someone uses your Social Security number to get a job. That employer will report that person’s earnings to the Internal Revenue Service (IRS). When you file your tax return, you won’t include those earnings. But, IRS records will show you failed to report all your income and you can expect to get a letter from the IRS.

- Someone uses your Social Security number and files a tax return in your name before you file, they may get your refund. When you file your own return later, IRS records will show the first filing and refund, and you’ll get a letter from the IRS.

If you think someone has misused your Social Security number to get a job or tax refund—or the IRS sends you a notice indicating a problem—contact the IRS immediately:

- at the number provided in the notice from the IRS;
- If instructed by the IRS, go to IDVerify.irs.gov.
- Complete IRS Form 14039, Identity Theft Affidavit
- Further information is available at [https://www.irs.gov/Individuals/Identity-Protection](https://www.irs.gov/Individuals/Identity-Protection)

**Medical ID Theft**

A thief may use your name or health insurance number to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.

If you suspect an identity thief has used your medical information, you should:

- Get copies of your medical records. Under federal law, you have a right to know what’s in your medical files.
- Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and anywhere you believe the thief has used your information. For example, if a thief got a prescription in your name, ask for the...
record from the pharmacy that filled the prescription and the health care provider who wrote the prescription. You may need to pay a fee to get copies of your records.

The medical provider or office that created the information must change any inaccurate or incomplete information in your files. They also should tell labs, other health care providers, and anyone else that might have gotten incorrect information. If an investigation doesn’t resolve your dispute, ask that a statement of the dispute be included in your record.

Child ID Theft

Theft of a child’s identity is growing rapidly, with some estimating that more than 10% of children have had their identity stolen. Because most children receive a social security number when they are born, and then don’t apply for credit for many years, they become an enticing target for identity thieves. With a date of birth and a social security number, these thieves can apply for credit cards, loans, and other government services or benefits.

How do you know if your child’s identity has been stolen?

- Your child begins to receive suspicious mail, like pre-approved credit cards and other financial offers normally sent to adults, in his or her own name.
- You try to open a financial account for him or her but find one already exists, or the application is denied because of a poor credit history.
- A credit report already exists in his or her name. If the child has one, he or she may have been targeted already, since only an application for credit, a credit account, or a public record starts the compilation of a consumer credit file.

A parent or guardian can check whether a minor child has a credit report if they think the child’s information is at risk or if their child is approaching the age when they might first seek employment or credit of any kind. To get a minor child’s credit report, a parent or guardian must contact the credit reporting companies and provide proof of identity and other documents, including a birth certificate and the child’s social security card. Contact information for the three major credit reporting agencies is included at the back of this publication.
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.
- **“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 and businesses** looking for purses, wallets, computers and digital devices, files containing personal and financial information.
- **Computer hackers “breaking into” business or personal computers** to steal private client files and personal financial information commonly known as a data breach.
- **Phony e-mail or “pop-up” messages** known as click bait, phishing, and spam 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 or download malicious software or malware.
- **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?

- **Collect government benefits in your name** by using your SSN to apply for a job or to obtain a tax return.
- **Drain your bank account** with electronic transfers, counterfeit checks, or your debit card.
- **Open a bank or credit account in your name** and write bad checks, make charges that never get paid off, which gets reflected on your credit report.
- **Use your name if they get arrested or for conducting illegal activity** such as drug purchases that could result in warrants being issued in your name or go on your permanent record.
- **Obtain a driver’s license or a job** with your personal information.
- **Buy a car or property** and use your information and credit history to get a loan for it.
- ** Obtain utility 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.
- You suddenly stop receiving regular bank or credit card statements.
- Personal information, credit cards, ATM cards, checks, or IDs have been stolen from you.
- You have issues filing your taxes with the IRS.
- You suspect someone has fraudulently changed your mailing address.
- 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’re arrested for a crime you didn’t commit.

You could be the victim of identity theft without noticing any of these things happening to you. It is always a good idea to keep a careful eye out for anything out of the ordinary by ordering your free credit report at least once a year from [www.annualcreditreport.com](http://www.annualcreditreport.com).
Identity Theft Victim’s Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit identitytheft.gov to use a secure online version that you can print for your records.

Before completing this form:
1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

(1) My full legal name: ________________________________________________  
First                  Middle               Last       Suffix

(2) My date of birth: __________________  
mm/dd/yyyy

(3) My Social Security number: ________-______-__________

(4) My driver’s license: _________      ___________________  
State             Number

(5) My current street address:  
____________________________________________________________________________  
Number & Street Name                          Apartment, Suite, etc.

(6) I have lived at this address since ____________________  
mm/yyyy

(7) My daytime phone: (____)___________________  
My evening phone: (____)___________________  
My email: ______________________________________

ID Theft
Report

FTC ID Theft Affidavit

Police Report

Identity Theft Repair Kit
Protecting your passwords

- Do not use common numbers (like birth dates, phone numbers, or social security numbers) or commonly chosen words (child’s name, maiden name, pet’s name) as passwords or PINs.
- Never share your passwords or PIN numbers with anyone, not even a child or a spouse.
- Don’t use the same passwords—or slight variations of the same passwords—for all of your computers and mobile devices, or for all of your online sites.
- Don’t keep a written list of your passwords in your desk, filing cabinet, or anywhere a thief is likely to look.
- Choose “strong” passwords comprised of a combination of numbers, uppercase letters, lowercase letters, and, if possible, other characters.
- There are a variety of password manager tools that can generate completely random passwords and store them for you in an encrypted format.
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.

**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.identitytheft.gov or by calling their toll-free number: 1-877-ID-THEFT (1-877-438-4338) or 1-866-653-4261 (TTY). 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 http://identitytheft.gov. 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
1-800-525-6285

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

**TRANSUNION**
www.transunion.com
childidtheft@transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289
Contact all three credit bureaus IMMEDIATELY.
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 canceled 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.

**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.

**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 [https://ribbs.usps.gov/locators/find-is.cfm](https://ribbs.usps.gov/locators/find-is.cfm).

**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: [https://www.socialsecurity.gov/forms/ssa-7050.pdf](https://www.socialsecurity.gov/forms/ssa-7050.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
http://www.travel.state.gov/passport
1-877-487-2778
1-888-874-7793 (TDD/TTY)

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, 1300 Broadway, 6th Floor, Denver, CO 80203, or call 720-508-6022. Additional information is available online at http://coag.gov/car/licensing.

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.
You can check your credit report online immediately at www.annualcreditreport.com.
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 can be limited to $50 in unauthorized credit card charges per card if you notify your bank or card issuer immediately. Notification more than 2 days and less than 60 days after discovery will cap your losses at $500. After that (notification is more than 60 days after discovery) your liability might be unlimited. 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.

**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 14), 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 [http://www.stopfraudcolorado.gov/fraud-center/identity-theft](http://www.stopfraudcolorado.gov/fraud-center/identity-theft).
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. Filled out the Identity Theft Affidavit.
☐ 3. Obtained a copy of your credit report.
☐ 4. 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.
☐ 5. Placed a fraud alert on your credit report.
☐ 6. Closed any accounts that might have been tampered with or opened without your knowledge or consent.
☐ 7. Contacted a major credit bureau by phone and by writing to correct inaccurate information.
☐ 8. Contacted the correct agencies to fix inaccurate information, close accounts, or report identity theft.

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
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 canceled 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 “Opt-Out” program. Call 1-888-5-“OPT OUT” (1-888-567-8688) or visit www.optoutprescreen.com 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 un-secured 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 cross-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. Send your name and address with a written request to:
DMA Mail Preference Service ATTN: Dept. 12059580
Direct Marketing Association
P.O. Box 282
Carmel, NY 10512

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.

Contacts

Colorado Attorney General’s Office

http://coag.gov
http://www.stopfraudcolorado.gov/
http://www.stopfraudcolorado.gov/fraud-center/identity-theft

Ralph L. Carr Colorado Judicial Center
1300 Broadway, 10th Floor
Denver, CO 80203
(720) 508-6000
Consumer Line: 1-800-222-4444

Federal Trade Commission (FTC)

https://identitytheft.gov

Consumer Response Center, Room 130-B
600 Pennsylvania Avenue N.W.
Washington, D.C., 20580
1-877-ID-THEFT (1-877-438-4338)
1-866-653-4261 (TTY)

Major Credit Bureaus

Equifax:
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-525-6285

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

TransUnion:
www.transunion.com
childidtheft@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:

Central Source LLC
P.O. Box 105283
Atlanta, GA 30348-5283
or call: 1-877-322-8228
TDD: 1-877-730-4104
Major Check Verification Companies

To request a copy of your consumer report specifically about your checking account: Chex Systems, Inc. at 1-800-428-9623 or https://www.chexsystems.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
http://www.socialsecurity.gov

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
SSA Fraud Hotline: 1-800-269-0271
1-866-501-2101 (TTY)

U.S. Postal Inspection Service
To find your local postal inspection office visit: https://ribbs.usps.gov/locators/find-is.cfm

Colorado Division of Motor Vehicles
Visit this website to find the DMV service center closest to you: https://www.colorado.gov/dmv