

## What to Do if You Have Become a Victim of Identity Theft

1. Call your credit card company or bank as soon as possible to report and dispute the fraudulent charges, and to close the affected account(s). The police will need any credit card statements, copies of checks, or other information you obtain for their investigation.

2. Report the crime to the local law enforcement agency where you reside. Have any documents or copies of documents available for the officer when making your report.

3. Call, or go online, to one of the three major credit reporting agencies to place a "fraud alert" or "credit freeze" on your name and social security number, and request a copy of your credit report:

**Equifax, [www.equifax.com](http://www.equifax.com), 1-800-525-6285**

**Experian, [www.experian.com](http://www.experian.com), 1-888-397-3742**

**TransUnion, [www.transunion.com](http://www.transunion.com), 1-800-680-7289**

4. Explore other options available to you:

a. Make an online identity theft report to the FTC at [www.ftc.gov](http://www.ftc.gov) or call 1-877-FTC-HELP.

b. Visit the Colorado Attorney General's Web site at [www.ago.state.co.us](http://www.ago.state.co.us) for an "Identity Theft Repair Kit."

c. Visit the JCSO website at [www.jeffcosheriff.com](http://www.jeffcosheriff.com) for more information on identity theft prevention.

*For more information on identity theft prevention, visit us online at [www.jeffcosheriff.com](http://www.jeffcosheriff.com)*



*As law enforcement professionals, we pledge to serve the Jefferson County community, build trust and confidence, and respond to community needs with:*

### Integrity

We interact with each other and the community we serve with honesty, dignity, and respect.

### Innovation

We respond to the community's needs with vision and initiative, relying on both traditional and non-traditional problem-solving methods.

### Partnership

We actively promote a spirit of teamwork and cooperation through open communication and the free exchange of ideas.

### Service

We continuously develop our skills and talents to provide top quality, responsive, effective law enforcement services.

### Accountability

We ensure judicious management of human, financial, and physical resources.

### Jefferson County Sheriff's Office

200 Jefferson County Parkway  
Golden, CO 80401

**Office Hours:** 8 a.m. - 5 p.m., Mon.-Fri.

Phone: 303.277.0211

Emergency: Dial 911

[www.jeffcosheriff.com](http://www.jeffcosheriff.com)

# Identity Theft



*It can happen to you.*



# Identity Theft

Identity theft involves the unauthorized use of another person's personal identifying information or financial identifying information to obtain cash, property, or services, or otherwise gain a benefit.

According to a report by the Federal Trade Commission, Colorado ranked #1 nationwide in the number of fraud and other complaints made in 2008. The same report showed that Colorado ranked tenth in the number of identity theft reports made in the same time period.

## Most Common Forms of ID Theft in Jefferson County

**Flagging** is placing the red flag on your mailbox in the up position to alert the mailman that there is

outgoing mail to be picked up. *This alerts identity thieves that there is information available to be stolen.*

**Skimming** is the practice of using a small electronic device to capture the information encoded in the electronic strip on the back of credit cards, debit cards, and driver's licenses. *Identity thieves can use skimmers to steal information in a variety of situations.*

**A trespass to a motor vehicle** involves someone breaking into a locked or unlocked vehicle to steal something of value. *Identity thieves often break into cars to steal visible wallets and purses, and use any credit cards or account information they find.*

**Phishing** is the deceptive use of e-mail messages, social networking sites, instant messaging sites or cell phone text messages to steal your personal data (date of birth, credit card information, PIN numbers, passwords and more!). You believe the request for information comes from a legitimate source, but the message is from the thief. The

message has been designed and written to appear to be from your financial institution. *Your bank will never send you a message via e-mail to ask you to verify or provide account information, but identity thieves use this form of deception to steal and use your information.*

**Social engineering** is the act of manipulating people into performing actions or divulging confidential information. The term applies to deception for the purpose of information-gathering or requesting money. Often seen in dating websites, a target victim will be set up by ongoing conversations with a person who seems legitimate, and who then asks for money to be sent to help them with a catastrophe of some sort, usually a hospital bill or something similar. Sometimes a victim will be targeted via telephone, and the target victim will believe they are speaking to a grandson or granddaughter who needs money to help them get home or out of jail. *These are identity thieves too!*

## HOW TO PREVENT IT FROM HAPPENING TO YOU

### Do

DO store your personal information in a safe place; i.e. in a locked cabinet or other locked location in your home.

DO shred credit card receipts, old bank statements, or any extraneous documents with your personal information.

DO protect your PIN and passwords.

DO remove your name from mailing lists for pre-approved credit offers and your phone number from telemarketers' lists. To opt out of pre-approved credit offers call 1-888-5-OPT-OUT and to place your number on the National Do Not Call Registry visit the website [www.donotcall.gov](http://www.donotcall.gov).

### Do

DO take your outgoing mail directly to the post office, or place your mail into a blue post office box.

DO check your credit card and bank account statements regularly.

DO request and review your credit report each year.

DO close all extraneous or unused credit card accounts and bank accounts. Keep only those accounts which you regularly use.

DO contact your creditor or service provider if expected bills do not arrive on time in the mail.

DO protect your mail from theft. Opt for replacing your old mailbox with a locking mailbox.

### Don't

DON'T give personal information to anyone via phone, mail or Internet, unless you initiated contact.

DON'T carry your social security card in your wallet.

DON'T write your PIN number on the back of your ATM or debit card.

DON'T leave your social security card, credit cards or identification cards in your vehicle.

DON'T pre-print checks with your social security number, driver's license number, or phone number.

DON'T choose PINs/passwords that are easy to guess. Create a PIN or password that contains a combination of numbers and letters.