We are here to serve you, when you need it the most!

17th Judicial District Attorney's Office:

(303) 659-7720

Email: da17@da17.state.co.us

Visit us at http://adamsbroomfieldda.org/

Follow us on social media for latest information:

Facebook: @da17colorado
Twitter: @da17colorado
Instagram: @da17colorado
YouTube: ColoradoDA17

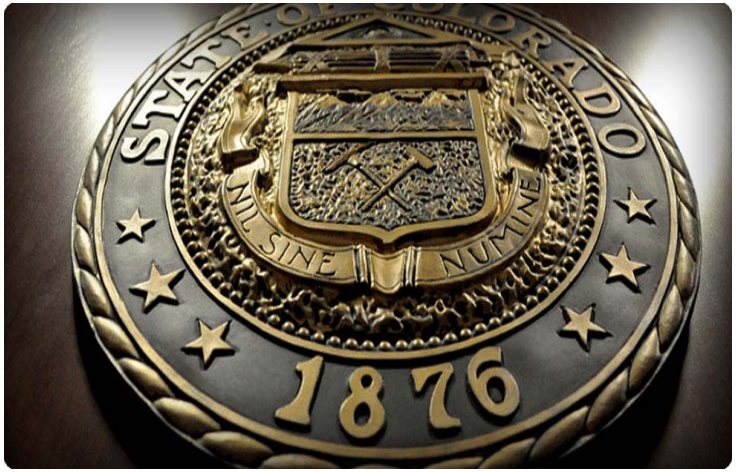
District Attorney Brian Mason

17th Judicial District Attorney's Office

Serving Adams and Broomfield Counties

District Attorney Brian Mason

Staying Safe from Identity Theft and Fraud: A Resource for Our Community



NOTES

Tips for Protecting Children

☐ **Set Privacy Settings On Their Devices**:

Apps and social networks are as customizable today as they can be. It's not too hard to figure out how to set these customizations, so you should learn them, and even explain them to your kid, if possible.

☐ **Make Your Child Anonymous Online**:

Fake personal info – dishonesty isn't recommendable in any form, but it's better than the consequences of giving away free data. Your child should know not to leave the real address, number, birthday date, and even a first and middle name is better than first and last.

Use ad blockers – ads online aren't just ads, but also data miners. And there are even the malicious ones, fake ones, and alike. Block them all, so your children can browse safely.

Anonymous search – just like you, your children will have to search the internet for things as well. If they use Google, most of their info will be recorded and added to their account. Google will do this for better ad targeting, and it won't allow your children's anonymity. Instead, they should use anonymous search engines like, StartPage or DuckDuckGo.

17th Judicial District Attorney's Office

Serving Adams and Broomfield Counties

District Attorney Brian Mason

Table of Contents

Facts About Identity Theft and Fraudulent Scams

- Identity theft is the fastest growing crime in America. Identity thieves are everywhere. Thieves are looking for checks, credit card "convenience checks," pre-approved credit card applications and statements in your mailbox and/or in your trash. Some may try to contact you through "phishy" e-mails or phone calls asking you to verify account numbers by impersonating your bank, credit card company, etc.

- Along with names, Social Security numbers, and dates of birth, fraudsters also use Medicare numbers, addresses, birth certificates, death certificates, passport numbers, financial account numbers (i.e., bank account, credit card), passwords (e.g., mother's maiden name, father's middle name), telephone numbers, and biometric data (e.g., fingerprints, iris scans) to commit identity theft.

- According to the Federal Trade Commission, identity theft complaints nearly doubled between 2010 and 2015. However, the number of identity theft victims and total losses are likely much higher than publicly-reported statistics.

- Con artists, sometimes known as "travelers," prey on older adults in both cities and rural communities with door-to-door roofing, painting and tree trimming scams. Although they quote bargain prices, the amount doubles or triples after the work (usually shoddy) is done.

- The majority of investment fraud cases involve financial advisors who have had long-term, trusting relationships with their victims.

- Many cases of theft involve family members or trusted advisors who take advantage of their victims who have given up full control of finances.

Cyber Safety Checklist

- ☐ Use **STRONG** Passwords and **CHANGE** them often.
- ☐ Have a **DIFFERENT** Password for each account.
- ☐ **UPDATE** apps and computer systems regularly.
- ☐ Install quality security (anti-virus, etc.) on **ALL** of your devices (including Smartphones).
- ☐ Use **2 STEP AUTHENTICATION** (2 Passwords to access).
- ☐ Know when you are using **PUBLIC WI-FI** and when you are using **PRIVATE WI-FI**.
- ☐ Use **PRIVATE WI-FI** for financial or personal transactions, and only in secure locations.
- ☐ **DO NOT** share too much information on social media.
- ☐ **DO NOT CLICK** on Ads.
- ☐ **ONLY** download verified Apps in the App Store or Google Play.
- ☐ Use **COMMON SENSE** regarding emails and texts from strangers.
- ☐ **NEVER** "Click Here."

Identity Theft & Fraud Prevention

- ☐ **REMOVE** anything with your Social Security number on it from your wallet or purse.
- ☐ **DO NOT** give personal information or financial information over the phone.
- ☐ **REPORT** any fraudulent activity or the loss or theft of your credit/ debit card or checkbook immediately.
- ☐ **SHRED** all documents containing personal information.
- ☐ Read all documents carefully **BEFORE** you sign.
- ☐ **DO NOT** wire funds to anyone who overpays for something sold on line or sends a check or money order then cancels the deal asking you to cash the check and wire money.
- ☐ Give checks or money orders you receive from strangers **TIME TO CLEAR** your accounts before you use the funds.
- ☐ Make a charitable giving plan and stick with it, donating only to charities you know and trust.
- ☐ **DO NOT** wire money to people you do not know.
- ☐ If a friend or family member requests a wire of money, check it out to make sure you are really sending money to your loved one.

Types of Identity Theft

Identity Theft:

All forms of Identity Theft involve using personal identifying information.
To understand the scope of Identity Theft, we talk about it in terms of the following types of Identity Theft.

Financial Identity Theft:

What most people think of first when thinking of Identity Theft. Defined as any form of Identity Theft which accesses a person's financial resources or credit.

Medical Identity Theft:

The use of another person's identifying information to obtain medical services, prescriptions or any other medical, psychiatric or substance abuse treatment.

Types of Identity Theft

Employment/Benefits Identity Theft:

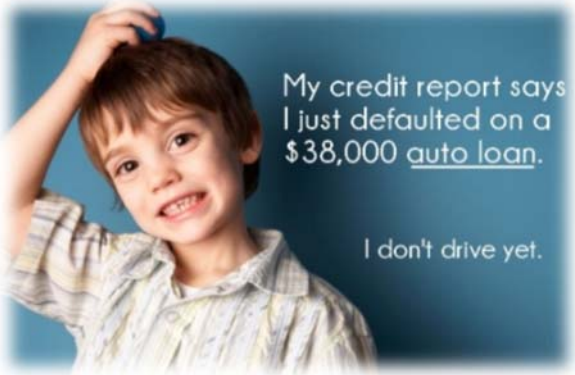
The use of someone's social security number to obtain employment, to claim public or veterans benefits or to apply for unemployment benefits.

Criminal Identity Theft:

This form of Identity Theft occurs when someone uses another person's identity when charged with a crime, arrested or given a traffic ticket.

Child Identity Theft/ At-Risk Adult Identity Theft:

Any form of Identity Theft which is perpetrated using the Identity of a minor child or of an older adult or person with a disability.



If you have been a victim or would like additional information,

please contact our office and/or the CBI Hotline

17th Judicial District Attorney's Office:

(303) 659-7720

Email: da17@da17.state.co.us

Victim Advocate 303-239-4242

CBI 24 Hour Hotline 1-855-443-3489 (toll free)

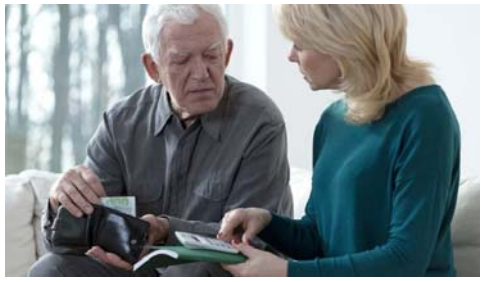
Protect The Elderly

WARNING SIGNS OF CAREGIVER FRAUD:

- Unusual activity in bank and credit card accounts.
- Caregiver tries to isolate the victim who comes to rely solely on the caregiver.
- Caregiver has total control over finances and has all financial statements mailed to him or her.
- New acquaintances appear on the scene and the adult is either completely charmed or fearful of the caregiver.

PREVENTATIVE STEPS:

- If your Power of Attorney or anyone else suggests you make a change in your assets, your investments, or insurance, always get two or three other opinions from within your team of advisors. Only a potential crook will not want you to discuss the change with others.
- No matter how much you know, love or trust someone, never sign papers you have not read or do not understand.
- Even if you have a representative payee, Power of Attorney or other advisor who manages your finances, insist on receiving and reviewing copies of all bank and financial statements.
- Please seek help from the courts to appoint a responsible and accountable fiduciary to help with managing finances and making financial decisions.



Types of Identity Theft

Domestic Violence/Elder Abuse/Stalking Identity Theft:

Any Identity Theft which is committed in conjunction with domestic violence, elder abuse, or stalking incident. This form of Identity Theft is often used by the perpetrator to intimidate and control the victim.

Tax Related Identity Theft:

The use of someone's social security number to file fraudulent tax returns and obtain fraudulent tax refunds.

Business Identity Theft:

The theft of a business by changing listings with the Secretary of State. This form of Identity Theft is committed to obtain credit, sell the business or set up fraudulent websites to divert business and online payments or to obtain personal information from customers.

Types of Fraud

- All forms of fraud have a common theme.
- Scams can be attempted with phone calls, letters, emails or text messages.
- Below are several common categories of fraud:
  - **Contractor Fraud –** Involves an untrustworthy and/or unreliable contractor that solicits services and collects money, but never completes work or performs work that falls well below the applicable standards/code.
  - **Telemarketing Fraud –** Deceptive and high-pressure tactics used by fraudsters that attempt to solicit money for services or donations over the phone.
  - **Mail Fraud –** Scams in the form of mass mailings meant to deceive people into sending money or personal information.
  - **Email Fraud –** Questionable emails designed to trick someone into making purchases/donations or allow access to sensitive and personal information.
  - **Title Fraud -** Home title fraud occurs when someone obtains the title of your property—usually by stealing your identity—to change ownership on your property title from your name to theirs and secure loans using your home as collateral.
  - **Investment Fraud –** Offers to invest in various seemingly lucrative investments that never pay off. Typical schemes are characterized by offers of low- or no-risk investments, guaranteed returns, overly-consistent returns, complex strategies, or unregistered securities.
  - **Caregiver/At-Risk Fraud –** Type of fraud occurs when the individual designated as a caregiver abuses the dependent through the misuse of a victim's property or financial resources without their consent or understanding.

Watch For Red Flags

- Suspicious Mail, Phone Calls, Text messages, or Emails, regarding loans or credit, which you did not apply for.
- Bills or collection notices for accounts which you do not own.
- Large number of credit inquiries on your credit report.
- New Credit Accounts appearing on your credit report.
- Calls, letters, or emails from a college or university about a financial aid package, which no one in your family is attending.
- **BEWARE** of outreaches offering to verify your breached identity or offering help to correct the damage.
- **DO NOT** click on links or open attachments. **DELETE** and **IGNORE**!

Resources

- **District Attorney's Office—** http://adamsbroomfieldda.org/
- **CBI Website—**www.colorado.gov/cbi
- **Federal Trade Commission (FTC)—**https://www.ftc.gov/faq/consumer-protection
- **FTC Identity Theft —**www.identitytheft.gov
- **Stop Fraud Colorado—**www.stopfraudcolorado.gov
- **Colorado Attorney General's Office—**www.coag.gov
- **Equifax—** www.equifax.com or call 1-800-685-1111
- **Experian—** www.experian.com or call 1-888-397-3742
- **TransUnion—**www.TransUnion.com or call 1-800-916-8800
- **Social Security Office—**www.ssa.gov
- **Fraud Alert—**https://www.consumer.ftc.gov/articles/0275-place-fraud-alert
- **Credit Freeze—**www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes

Be Aware: Popular Scams

Money Wiring Scams

- The scam artist tries to scare or intimidate the victim into sending money immediately through a wire service (like Western Union or Money Gram), by an electronic funds transfer or through the purchase of a pre-paid credit card or gift card.
- This type of scam also includes calling and pretending to be a loved one in distress and needing money, contacting the victim and claiming to be with a government or law enforcement agency collecting a fine or debt, or representing one's self as an IRS agent calling about past due tax debt.
- Another way this scam is being committed is through online-sales or offers of jobs like a personal assistant or mystery shopper.
- All of these scams have one thing in common, to ask the victim to send money to another person.
- Once the victim has sent the money, additional requests for funds will follow, with the callers becoming more aggressive and even threatening.

Be Aware: Popular Scams

Lottery Scams

- You have won $2 million! All you have to do to claim your prize is pay some type of tax or processing fees.
- Many people will send these criminals thousands of dollars in the hopes of getting millions.
- But in the end, it is just a scam. Sometimes, the criminals in this scam will ask for the victim's bank account information so they can transfer funds into the account.
- What they will really do is use the information to wipe out the victim's bank account.

Investment Scams

- Watch out for high pressure sales tactics with an insistence on an immediate decision.
- Always discuss the deal with another advisor or get a second opinion from a trusted friend or family member.
- Be wary of a guaranteed investment or one with "no risk."
- All legitimate broker/dealers must provide written information, including state securities registrations and verifiable references.
- Thoroughly check out any offer. Don't let yourself be rushed into making a hasty decision. Contact the Colorado Division of Securities at 303-894-2320 if you have any questions.
- Carefully review your financial statements.

Know Your 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 bank marketing programs, including "convenience checks" sent on your credit card account. Call the company's customer service numbers to Opt Out (see pg. 16).
- 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.

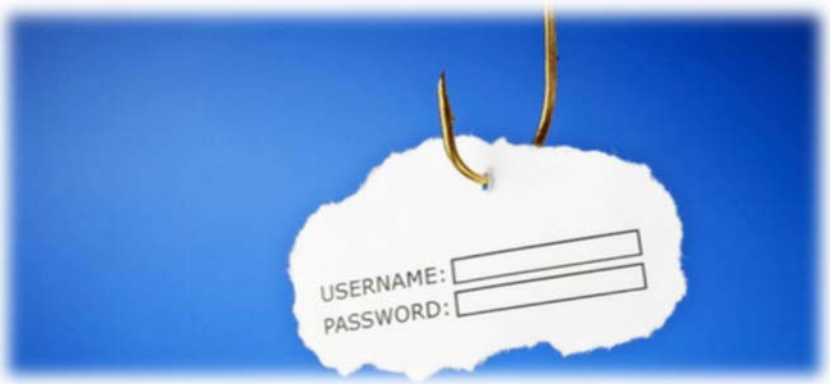
UNDER COLORADO LAW, YOU HAVE THE RIGHT TO:

- 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 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 SSN printed on 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.

Cyber Security - Identity Theft Prevention Tips

Be careful with your online and phone activity

- **DO NOT GIVE OUT PERSONAL INFORMATION**, such as your name, birthdate, social security number, or bank account number online.
- **DO NOT SHARE** your online passwords with anyone.
- **DO NOT** share personal information over the phone with someone you do not know.
- Do not use the same username and password for all your online account log ins.
- Create a **STRONG** password which contains multiple types of characters, numbers, letters, and symbols.
- **PUBLIC WIFI** is not as secure as your own **PRIVATE WIFI**.
- Be aware of **PHISHING SCAMS**, e.g. Click Here!, Download This!
- **DO NOT** click on Ads.
- If you do not know who sent you an email or text, proceed with **CAUTION**.



Be Aware: Popular Scams

Romance Scams

- Millions of Americans participate in online dating and expose themselves to a large number of scam artists.
- Many scams leverage someone's personal feelings into requests for money or personal loans that are never repaid.
- Some scam artists will ask for money to help travel to meet in person, but take money and disappear.
- These scams can devastate a victim financially and emotionally.

Contractor Scams

- Be wary of unlicensed contractors soliciting you at your door, insisting that you have structural problems on your home which must be repaired right away.
- Be wary of contractors offering unusual bargain prices or claiming to have materials left over from another job.
- Don't work with a contractor that requires a substantial payment in advance or charges significantly more after the work is complete.
- Get at least three written bids. Don't always choose the lowest bidder. Almost all complaints to the DA's office involve contractors with very low bids. Remember, you get what you pay for.
- Require the contractor to use a *written* contract that lists detailed work descriptions, materials, costs, and the completion date.

Identity Theft Prevention Tips

Guard your Social Security number

- Do not carry your Social Security card or your birth certificate in your wallet or purse. Be cautious with Military Identity cards, replacing any cards, which still include your Social Security number.
- **NEVER** give your Social Security number to someone you do not know and trust.
- **ALWAYS** ask why it is needed, if someone requests your Social Security number. Some agencies (like the IRS or credit reporting bureaus) will need it, but most do not.

Identity Theft Prevention Tips

Review your credit report on a regular basis

- You may request a **FREE** credit report from each of the three major credit reporting bureaus once a year.
- An Annual Credit Report Request is a free service recommended by the Federal Trade Commission, as a safe and reliable source. Contact them for copies of your credit report at: www.annualcreditreport.com or by calling 1-877-322-8228.
- Review your credit report and contact the credit reporting bureau, if there is anything on the report, which does not belong to you .
- If you have concerns, consider a Fraud Alert or Credit Report Freeze.

OPT OUT

- Consider Opt-Out options for credit card solicitations, credit card convenience checks and junk mail. Visit www.optoutprescreen.com or call 1-888-5-OPT-OUT (1-888-567-8688)

Get Additional Information

- Contact the Colorado Bureau of Investigation if you would like to learn more or if you are interested to discuss a personal crime prevention plan.

Call the Experts

CBI Identity Theft & Fraud

24 Hour

Hotline 1-855-443-3489 (toll free)

Identity Theft Prevention Tips

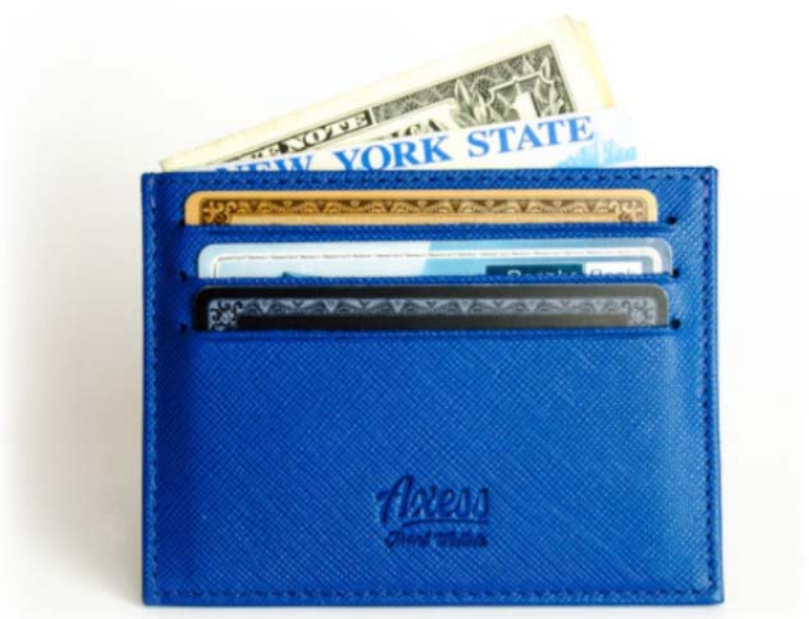
Be careful with mail and other documents

- Bring mail in as soon as possible and consider a locking mailbox.
- Shred all mail and other documents which contain personal identifying information. A cross-cut shredder is best.
- Take any mail which contains checks, credit card information or other personal identifying information to the Post Office to mail rather than leaving it in a mailbox to be picked up.
- Ask your financial institution to have new checks or debit cards delivered to them and go in to pick them up.
- When giving a loved one a gift of cash, consider sending a gift card instead of a check or money order.
- Keep Social Security cards, Medicare cards, extra Military Identity cards, copies of tax returns, statements, bills and other critical information in a safe place in your home—preferably in a locked container.
- **NEVER** sign a document you have not read or do not understand.
- Seek the advice of a professional before naming an agent on a Power of Attorney to ensure you understand how much control the agent will have to make decisions for you.

Identity Theft Prevention Tips

Reduce the items you carry in your wallet or purse

- Leave extra credit cards and the checkbook at home and carry only what you need with you.
- Consider downsizing to a close-fitting or neck pouch or carrying your wallet in a front pocket.
- Copy the front and back of everything you carry in your wallet and keep in a safe place at home for reference.



Identity Theft Prevention Tips

Be careful with Credit/Debit Cards and Bank Account information

- **NEVER** give your credit or debit card to someone else to use.
- If someone calls, emails or sends a text message saying they are with your credit card company or bank, they should already know your account numbers. **DO NOT** give out those numbers to the caller. Hang up and call your financial institution using the number printed on the card.
- Carefully review your credit card and bank statements every month to ensure everything listed is a legitimate charge. Call **IMMEDIATELY** if you see anything questionable, even if it is only for $1.
- If you lose your credit card, debit card or checkbook, contact your financial institution right away and report it missing.
- Consider asking your Financial Institution for a Fraud Alert to be placed on your accounts, so you will be notified of any unusual charges.
- Let your credit card companies and bank know if you plan to travel and where you will be going. They will be able to look out for unusual card uses if they are informed ahead of time.
- Consider bank issued prepaid credit cards for travel and children in college.
- Pay inside when getting gas instead of using pay at the pump.
- Pay with a credit card instead of a debit card to protect your bank account.

Identity Theft Prevention Tips

Be careful with Credit/Debit Cards and Bank Account information, continued...

- Be cautious when using an ATM machine, check the ATM for any signs of tampering.
- Try to use ATMs which are located at your bank, attached to the bank or in the bank lobby.
- Whenever possible, conduct bank business during business hours in the bank.
- Shield your hand when entering your PIN to prevent onlookers or hidden cameras from recording you PIN number.
- If your credit or debit card is stolen or compromised in any way, report it to the police and to your financial institution right away. You must act quickly to protect your accounts.
- Remember: **NEVER** give out your PIN number.