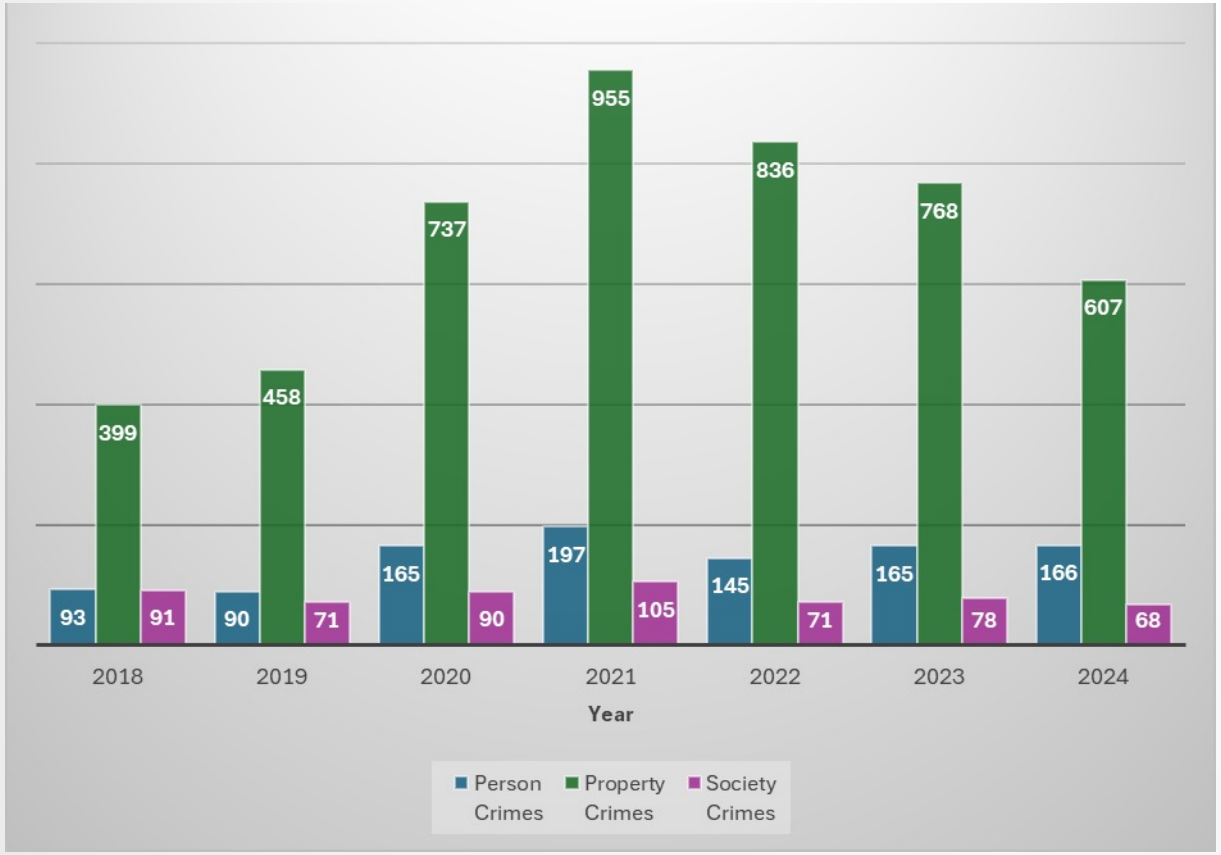
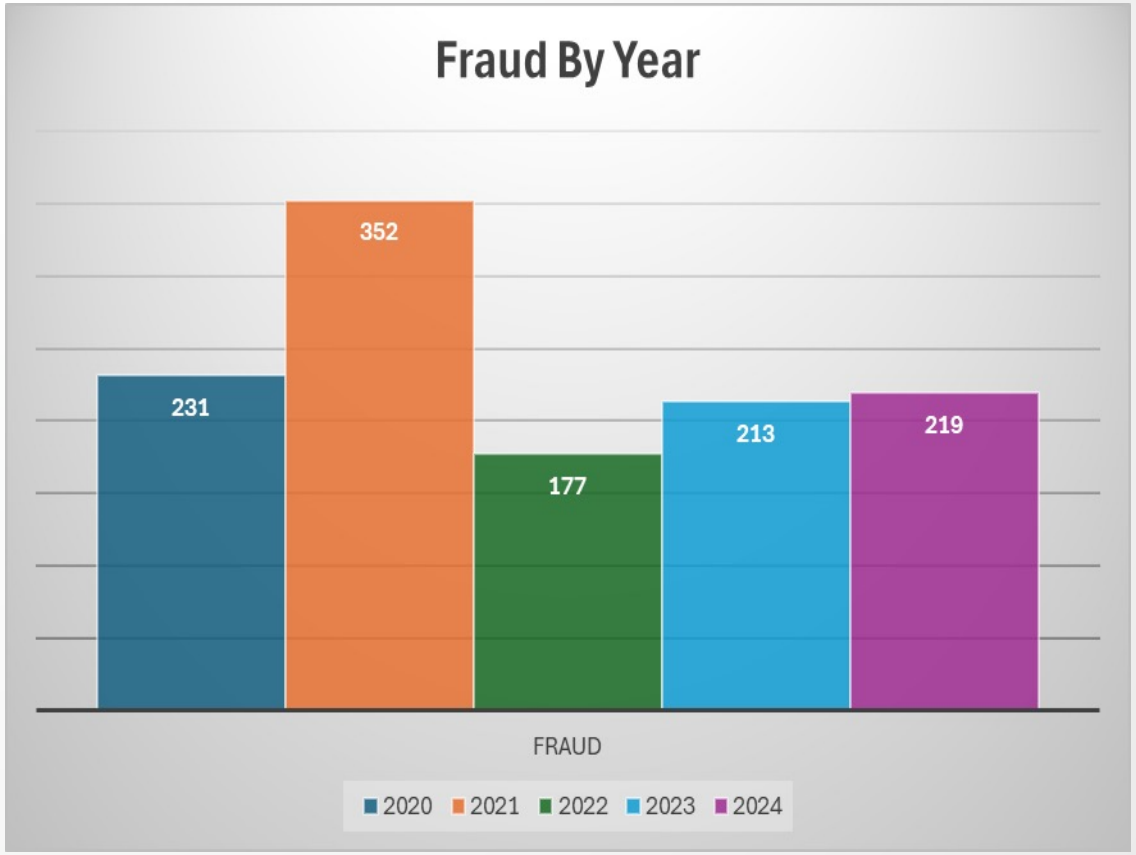
Fraud & Scams Targeting Colorado

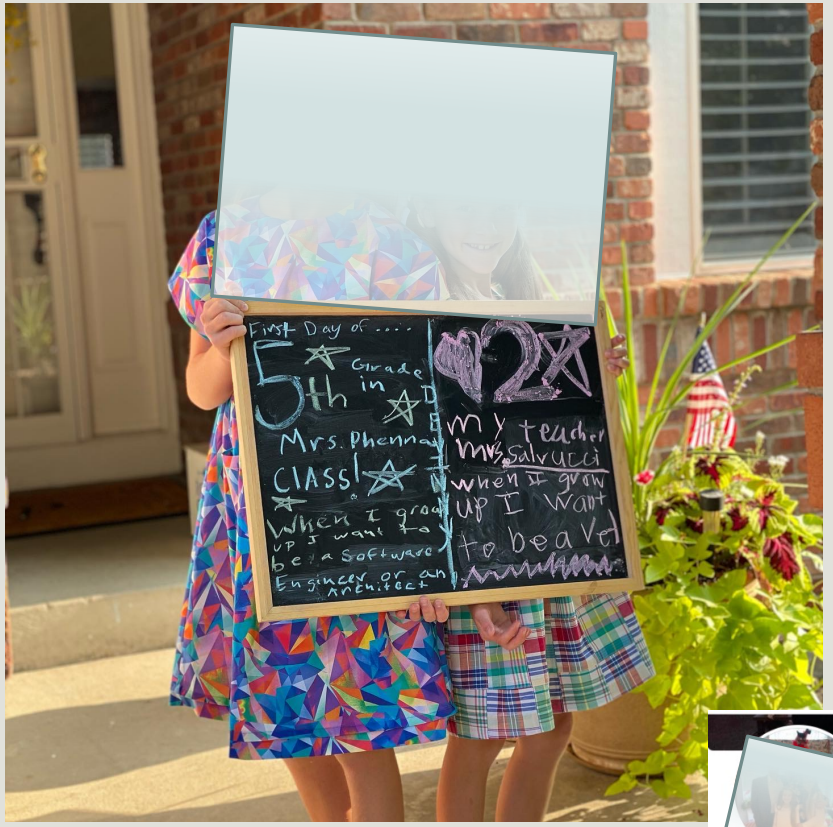
Presented by: Scott Moore
Crime Prevention Specialist
Louisville Police Department
SMoore@LouisvilleCO.gov
303-335-4688

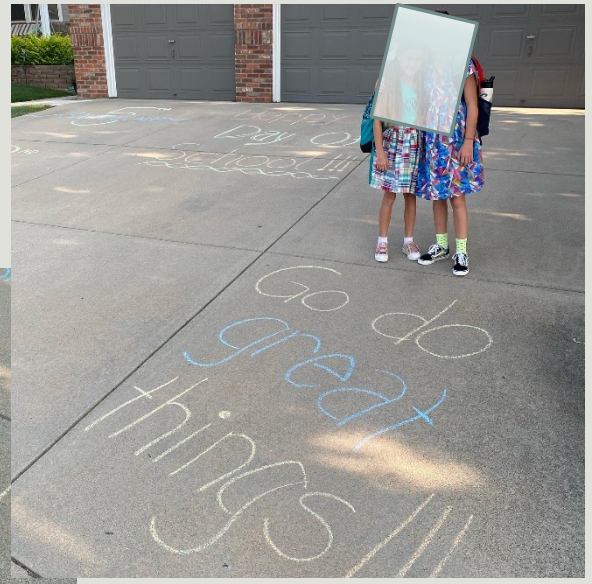
Crime Statistics
Louisville, Colorado

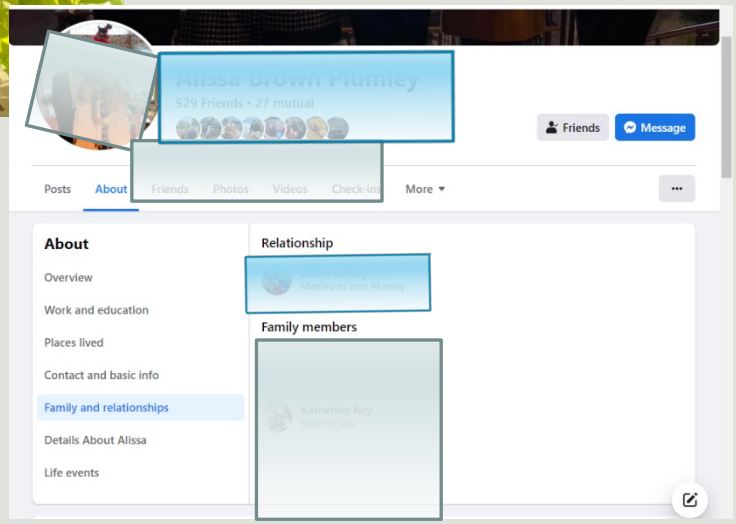




WHEN IT COMES TO FRAUD, WE DON'T WANT TO BE THE ONE THAT STANDS OUT IN THE CROWD







LOUISVILLE POLICE Colorado

Colorado is estimated to be the state with the highest rate of elder fraud in the United States

- 272,900 older adults fall victim to elder fraud each year
- an estimated $2.75 billion a year is lost through scams
- Fraud among older adults can come from a variety of places including strangers and family
- 300-400 calls a month are made to AARP ElderWatch Fraud Line

Why are older adults targeted for financial fraud and scams?

- More Trusting
- Seen As Having Wealth
- May Be Isolated
- Seen As Not Being Technology Capable
- Potential Health/Memories Concerns

Common Scams Targeting Colorado

1. Imposter Government (mostly SSA)
2. Sweepstakes/Prize/Lottery
3. Internet & Computer Virus Fraud
4. Home Repair & Improvement
5. Phishing
6. Romance/Online Dating
7. Identity Theft
8. The Grandparent Scam
9. Elder Financial Abuse
10. Charity Scams

Imposter Government (SSA) Scam

- Often starts with a call, email, or text
- Imposter says they're with a government agency.
  - might give you their "employee ID number"
  - might have information about you, like your name or home address
- Often say they work for the Social Security Administration, the IRS, or a law enforcement agency
- Give a reason why you need to send money or give them your personal information immediately.

If you get a call like this, hang up the phone. It's a scammer. Government agencies won't call, email, or text you and ask for money or personal information. Only a scammer will do that.

How To Avoid Imposter Government (SSA) Scam

•**Don’t wire money, send cash, or use gift cards, gold or cryptocurrency to pay someone who says they’re with the government.** Scammers ask you to pay these ways because it’s hard to track that money, and almost impossible to get it back. They’ll take your money and disappear.

•**Don’t give your financial or other personal information** to someone who calls, texts, or emails and says they’re with the government. If you think a call or message could be real, stop. Hang up the phone and call the government agency directly at a number you know is correct.

•**Don’t trust your caller ID.** Your caller ID might show the government agency’s real phone number or even say “Social Security Administration,” for example. But caller ID can be faked. It could be anyone calling from anywhere in the world.

•**Don’t click on links in unexpected emails or text messages.** Scammers send emails and text messages that look like they’re from a government agency, but are designed to steal your money and your personal information. Don’t click on any link, and don’t pass it on to others. Simply delete the message.

Sweepstakes/Prize/Lottery Scam

- Scammers inform you that you have won a lottery or sweepstakes
- Say you need to make some sort of payment to unlock the supposed prize
- May send a check that they can deposit in your bank account, knowing that while it shows up in their account immediately, it will take a few days before the (fake) check is rejected.
- Criminals will then collect money for supposed fees or taxes on the prize
- victim has the “prize money” removed from his or her account as soon as the check bounces

How To Avoid Sweepstakes/Prize/Lottery Scam

•**Real sweepstakes are free and by chance**. It's illegal to ask you to pay or buy something to enter, or to increase your odds of winning.

•**Contest promoters might sell your information to advertisers**. If you sign up for a contest or a drawing, you're likely to get more promotional mail, telemarketing calls, or spam.

•**Contest promoters have to tell you certain things.** If they call you, the law says they have to tell you that entering is free, what the prizes are and their value, the odds of winning, and how you'd redeem a prize.

•**Sweepstakes mailings must say you don't have to pay to participate.** They also can't claim you're a winner unless you've actually won a prize. And if they include a fake check in their mailing, it has to clearly say that it's non-negotiable and has no cash value.

Internet & Computer Virus Fraud

Phone calls

- Tech support scammers call and pretend to be a computer technician from a well-known company.
- They say they've found a problem with your computer.
- They often ask you to give them remote access to your computer and then pretend to run a diagnostic test.
- Then they try to make you pay to fix a problem that doesn't exist.

Pop-up warnings

- Tech support scammers try to lure you with a pop-up window that appears on your computer screen.
- It might look like an error message from your operating system or antivirus software, and it might use logos from trusted companies or websites.
- The message in the window warns of a security issue on your computer and tells you to call a phone number to get help.

How to Avoid
Internet & Computer Virus Fraud

- If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up
- If you get this kind of pop-up window on your computer, don't call the number. Real security warnings and messages will never ask you to call a phone number.
- Legitimate tech companies won't contact you by phone, email or text message to tell you there's a problem with your computer
- Security pop-up warnings from real tech companies will never ask you to call a phone number

Home Repair & Improvement Scams

- Someone knocks on your door or calls you.
- They say they can fix your leaky roof, install new windows, or provide the latest energy-efficient solar panels.
- They might find you after a flood, windstorm or other natural disaster.
- They pressure you to act quickly, might ask you to pay in cash, or offer to get you financing.
- They run off with your money and never make the repairs, or they do shoddy repairs that make things worse.
- They may even put you in a bad financing agreement that puts your house at risk.

How to Avoid
Home Repair & Improvement Scams

- **Stop. Check it out**. Before making home repairs, ask for references, licenses and insurance. Get three written estimates. Don't start work until you have a signed contract. And don't pay by cash or wire transfer.

- **Pass on this information to a friend.** You may see through these scams. But chances are you know someone who could use a friendly reminder.

Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information.
They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts.

Phishing emails and text messages may look like they're from a company you know or trust.
They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff

Steps To Protect Yourself From Phishing

1. **Protect your computer by using security software**. Set the software to update automatically so it can deal with any new security threats.

2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

- Something you have — like a passcode you get via an authentication app or a security key.
- Something you are — like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

Romance/Online Dating Scams

- Professes love quickly. Claims to be overseas for business, military service, or other reasons they cannot physically meet.
- Asks for money, and lures you off the dating site.
- Claims to need money for - emergencies, hospital bills, business costs, or travel.
- May say they plan to visit, but give excuses why they cant.

How to Avoid Romance/Online Dating Scams

- **SLOW DOWN** and talk to someone you trust. Don't let a scammer rush you.
- **NEVER TRANSFER MONEY** from your bank account, buy gift cards, or wire money to an online love interest. You wont get it back.
- **CONTACT YOUR BANK & Police** right away if you think you have sent money to a scammer.

Identity Theft Fraud

Common ways that identity theft/fraud is committed

1.Looking over people's shoulders as they punch in their bank card numbers or listening to people give their information over the phone for things such as car rentals or hotel booking.

2.Searching through garbage for documents with your information and activating "pre-approved" credit cards.

3.Intercepting/stealing mail then redirecting it to the thief's address.

4.Your social security number may be stolen by means of

- Stealing information you provide to an unsecure website, documents at your job or home.
- Buying information from an inside source such as an employee at a bank, store, or another company that has your information.
- Theft of the actual Social Security card.

What To Do When Identity Fraud Occurs

Step 1: Call the companies where you know fraud occurred.

- Call the fraud department. Explain that someone stole your identity. Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
- Change logins, passwords, and PINs for your accounts.

Step 2: Place a fraud alert and get your credit reports.

- To place a free fraud alert, contact one of the three credit bureaus. That company must tell the other two.
  Experian.com/help 888-EXPERIAN (888-397-3742)
  TransUnion.com/credit-help 888-909-8872
  Equifax.com/personal/credit-report-services 800-685-1111
- Get updates at IdentityTheft.gov/creditbureaucontacts.
- Get your free credit reports from Equifax, Experian, and TransUnion. Go to annualcreditreport.com or call 1-877-322-8228.
- Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the Louisville Police.

Step 3: Report identity theft to the FTC.

- Go to IdentityTheft.gov, and include as many details as possible.

The Grandparent Scam

•A grandparent receives a phone call (or sometimes an e-mail) from a "grandchild." If it is a phone call, it's often late at night or early in the morning when most people aren't thinking that clearly. Usually, the person claims to be traveling in a foreign country and has gotten into a bad situation, like being arrested for drugs, getting in a car accident, or being mugged…and needs money wired ASAP. And the caller doesn't want his or her parents told.

•Sometimes, instead of the "grandchild" making the phone call, the criminal pretends to be an arresting police officer, a lawyer, a doctor at a hospital, or some other person. And we've also received complaints about the phony grandchild talking first and then handing the phone over to an accomplice…to further spin the fake tale.

•We've also seen military families victimized: after perusing a soldier's social networking site, a con artist will contact the soldier's grandparents, sometimes claiming that a problem came up during military leave that requires money to address.

How to Avoid
The Grandparent Scam

•Resist the pressure to act quickly.

•Try to contact your grandchild or another family member to determine whether or not the call is legitimate.

•Never wire money based on a request made over the phone or in an e-mail...especially overseas. Wiring money is like giving cash—once you send it, you can't get it back.

Elder Financial Abuse

Red flags to watch out for:

- Sudden changes in bank accounts or banking practices
- Unusual use of credit cards
- Telephone, water, electricity or other utilities being shut off
- Unpaid bills, liens or foreclosure notices despite sufficient income
- Checks written to "cash" or unauthorized ATM withdrawals
- Turning over finances or transferring assets to others without explanation or consent
- Disappearance of cash, valuable objects or financial statements
- Unexplained changes to wills or other financial documents
- Sudden changes in an elder's mood or demeanor

Preventing Elder Financial Abuse

•**Reduce the opportunity for phone scams.** Register with the national Do Not Call registry. Visit www.DoNotCall.gov or call 1-888-382-1222 from the phone number you wish to register.

•**Seek outside perspectives.** Consult with an attorney or trusted family member before making a large investment or purchases.

•**Protect personal information.** Shred bank documents, credit card receipts and financial records before throwing them in the trash.

•**Run a background check.** If you're hiring in-home care or a personal assistant, properly screen the person with a background check.

•**Use technology to stay connected.** Consider enrolling in mobile banking notifications to alert you every time a transaction is made or whenever their balance falls below a certain amount. This can help you identify charges you didn't authorize.

Charity Scams

- Fake charity scams prey on your goodwill and generosity.
- Scammers might pretend to be representatives of a legitimate charity.
- They'll call you, email you, or approach you on the street for donations.
- When you give, it’s likely your money will end up in the scammers’ pockets and not with the charity you were hoping to support.

Other scammers will make up their own charity names. They might even set up fake websites that look much like the sites run by legitimate charitable organizations. The goal, again, is to get you to make a donation not to a real charity, but to them.

How to Avoid Charity Scams

- **Donate to trusted, well-known charities**. Beware of scammers who create fake charities. Always verify a charity's legitimacy through its official website. If you have doubts, you can check with Better Business Bureau's Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar.
- **Verify all phone numbers for charities**. If you need to contact a charity by phone, check the charity's official website to see if the number you have is legitimate. If you're using text-to-donate, check with the charity to ensure the number is legitimate before donating.
- **Do not open suspicious emails**. If you receive a suspicious email requesting donations or other assistance, do not click on any links or open any attachments. Scammers regularly use email for phishing attacks and to spread malware.
- **Verify information in social media posts**. Double-check any solicitation for charitable donations before you give. Crowd-funding (ex: GoFundMe) websites often host individual requests for help but they are not always vetted by the site or other sources.

Annual Credit Reports

- Order your credit reports online at www.annualcreditreport.com.
- Different than a credit score!
- Credit reports can affect your mortgage rates, credit card approvals, apartment requests and job applications.
- Reviewing credit reports helps you catch signs of identity theft early.
- Check that all the information on your credit reports is correct and up to date.
- Dispute any incorrect information.

Credit Freezes and Fraud Alerts

- Credit freezes allow you to restrict access to your credit report, making it more difficult for identity thieves to open new accounts in your name.
- A credit freeze does not affect your credit score, keep you from opening a new credit account or prevent you from getting a free annual report.
- A freeze remains in place until you ask for it to be removed (using a PIN).
- Contact all three credit bureaus to place a freeze on your account
- A fraud alert protects your credit from unverified access for one year, you only need to contact one credit bureau to initiate this process.
- Both a fraud alert and credit freeze are FREE!

General Reminders for Avoiding Scams

- Protect your personal and financial information
- Speak with a vetted financial advisor about
- Manage your phone calls
- Do your research
- Avoid contact with any unknown entities (it’s OK to be skeptical or rude)
- Don’t rush to act (THINK!) and talk to others
- Consider unusual payment options a “red flag”
- Does it sound too good to be true?
- Actively seek information about trending scams/fraud
- Share your story
- Report!

Reporting

- Colorado Attorney General – www.stopfraudcolorado.gov
- Colorado Attorney General's Consumer Complaint Line – 800-222-4444
- Federal Trade Commission – www.ftccomplaintassistant.gov / www.identitytheft.gov
- FBI – www.ic3.gov
- Louisville Police Department 303.441.4444 (non-emergency) 911 (emergency)
- Local Better Business Bureau

Resources

Colorado Attorney General – www.stopfraudcolorado.gov / www.coag.gov

AARP – www.aarp.org/fraud

Federal Trade Commission – www.ftc.gov / www.identitytheft.gov


QUESTIONS