

Chapter 11

Arm Yourself with Consumer Protection Information

Amy Nofziger, M.A.*
AARP Foundation

Barbara Martin-Worley, M.A.*
18th Judicial District Attorney's Office

SYNOPSIS

- 11-1. Recognize — Refuse — Report
 - 11-2. Identity Theft
 - 11-3. Consumer Fraud
 - 11-4. Other Types of Financial Fraud
 - 11-5. Prevention Tools and Consumer Protections
 - 11-6. Resources
- Exhibit 11A. Sample Letter for Credit Freeze Request

11-1. Recognize — Refuse — Report

Financial exploitation cannot be completely prevented, but we want to empower you as consumers and educate you on how to Recognize, Refuse, and Report frauds in Colorado. It is the goal of this chapter to help you (1) learn the red flags of fraud; (2) recognize when someone is trying to victimize you; (3) learn when to say “no” and close the door or hang up the phone; (4) know how to report fraud to the appropriate agencies; and most importantly, (5) empower yourself. We value educating seniors because we know that education is the most important thing in preventing consumer fraud.

11-2. Identity Theft

Identity Theft

Identity theft is the fastest growing category of crime. Criminals, using a variety of methods, steal personal information from victims, including bank account, credit card, and Social Security numbers; driver's licenses; bank cards; telephone calling cards; and other key pieces of individuals' financial identities. Criminals use this information to impersonate victims, spending as much money as they can in as short a period of time as possible. Victims, faced with a damaged financial reputation and bad credit reports, spend months or even years trying to regain their financial health.

To protect against identity theft:

- ▶ Carry important documents in a close-fitting pouch instead of a purse that can be easily snatched or a wallet in your back pocket.
- ▶ Don't leave your purse unattended for even a moment in a grocery cart, restaurant chair, or other public areas.
- ▶ Do not carry extra credit cards, your checkbook, birth certificate, or passport in your wallet or purse. Carry your Medicare card only when you are obtaining health services.
- ▶ Protect your Social Security number (SSN). Don't carry your Social Security card with you.
- ▶ Don't have your SSN printed on your driver's license or checks.
- ▶ Don't give any part of your SSN or credit card number over the phone, unless you have initiated the call. One ploy criminals use is to call and pose as your bank or business and ask to "confirm" your SSN or other data.
- ▶ Shred pre-approved credit card offers and any papers that have your personal information using a cross-cut or confetti shredder.
- ▶ Never put your account number on an envelope or postcard.
- ▶ Keep a record of your credit card numbers, expiration dates, and customer service phone numbers.
- ▶ Do not pay bills by leaving the envelope, with a check enclosed, in your mailbox for carrier pickup; instead, drop off bills at the post office or pay your bills online.
- ▶ Have new boxes of checks sent to your bank or credit union rather than having them mailed to your home. Boxes of new checks are often stolen from mailboxes.
- ▶ Tell your credit card issuers to stop their marketing programs, including credit card convenience checks.
- ▶ "Opt out" of credit card solicitations by calling (888) 5-OPTOUT (567-8688). One contact will cover all three credit reporting agencies.
- ▶ Do not use common numbers (for example, birthdays or part of your social security number) or commonly chosen words (for example, a child's, spouse's, or pet's name) as passwords or PINs.

- ▶ Make certain that passwords are at least 13 characters or longer, and change passwords frequently if you do a lot of business over the internet — see “Cyber Crimes” under section 11.3, “Consumer Fraud.”
- ▶ Open credit card billing statements promptly and compare them with your receipts. Immediately report all discrepancies in writing. Under the federal Fair Credit Billing Act (FCBA), the card issuer must investigate billing errors if you report them within 60 days of the date your card issuer mailed you the statement.
- ▶ If you report the loss of your credit card before the card is used, the card issuer cannot hold you responsible for any unauthorized charges. If a criminal uses your card before you report it missing, your maximum liability will be \$50.
- ▶ Request a free copy of your credit report once a year from the three major credit reporting companies: (877) 322-8228 or online at www.annualcreditreport.com.
- ▶ Do not allow anyone to come into your home to use the phone or get a drink of water, as he or she might be setting you up for a robbery.

If you think your identity has been stolen:

- ▶ Immediately file a report with the police, U.S. Postal Inspection Service, or the district attorney. You will need a copy of the police report or affidavit as proof that you were a crime victim. A new resource that is now available through the Federal Trade Commission is the Identity Recovery Plan. It’s a personalized plan that helps you report and recover from ID theft. Visit <https://identitytheft.gov/> for more information.
- ▶ Contact the fraud departments of any one of the three major credit reporting companies and ask them to put a fraud alert on your account: Equifax, (888) 766-0008; Experian, (888) 397-3742; TransUnion, (888) 909-8872.
- ▶ Send a copy of the report or affidavit to your creditors and the credit reporting companies. Under Colorado law, once they receive your report or affidavit, they cannot put negative information in your credit file. Close any accounts that you think have been taken over or opened fraudulently. Get new cards with new account numbers. If you notice any irregularities on a bank statement, immediately notify your bank. You may need to cancel checking and savings accounts and open new ones.
- ▶ Call your utilities, especially cell phone service providers. Tell them someone may try to get new service using your identification.
- ▶ Review the information available online on the Colorado Attorney General’s website at <https://coag.gov/> or call (800) 222-4444 and ask for an Identity Theft Repair Kit.

Credit Repair

Newspapers, magazines, and the internet are filled with ads offering to erase negative information in your credit file. The scam artists who run these ads can’t deliver. Only time, diligent effort, and a debt repayment plan can improve your credit.

Your only choice is to help yourself re-build a better credit record. Start by contacting your creditors when you realize that you are unable to make payments. If you need help working out a payment plan and a budget, contact Money Management International at www.moneymanagement.org. Their services are free.

Credit Reporting Companies

Equifax

To order a credit report by:
Phone, (800) 685-1111
Internet, www.equifax.com
Mail, P.O. Box 740241
Atlanta, GA 30374

Experian

To order a credit report by:
Phone, (888) 397-3742
Internet, www.experian.com

TransUnion

To order a credit report by:
Phone, (800) 888-4213
Internet, www.transunion.com
Mail, P.O. Box 1000
Chester, PA 19016

Debt Collectors

If you cannot make your credit payments, the seller, loan company, or bank may give your debt to a lawyer or collection agency. These debt collectors can use any legal means to collect money you owe.

The federal Fair Debt Collection Practices Act and the Colorado Fair Debt Collection Practices Act control debt collectors' activities. They cannot do the following:

- ▶ Continue calling or writing after you tell them, in writing, that you do not want to be contacted;
- ▶ Call your friends or neighbors;
- ▶ Contact you or your boss at work if the collection agency knows your boss prohibits these types of calls;
- ▶ Call you before 8:00 a.m. or after 9:00 p.m., or use harassment or scare tactics;
- ▶ Threaten to file criminal charges against you, take your property, or garnish your wages without first filing a lawsuit to give you a chance to defend yourself (*Note: A lawyer acting as a debt collector cannot threaten criminal prosecution*); or
- ▶ Threaten you with any physical harm.

Debt Collection in Court

If you owe money to a creditor, he or she usually has the right to demand that you make payment in full.

If you miss a payment, pay less than the agreed amount, are late on a payment, or do something else that violates a written contract regarding the payments, the seller or creditor may have the right to demand payment of the full balance you owe on the debt. In this case, the creditor also may have the right to repossess the item you are making payments on.

If a loan company, bank, collection agency, or creditor decides to sue you, you must first be served with a summons to appear in court and a complaint that states why you are being sued. If you do not appear or respond, the other party may obtain a “default judgment” against you. This means the court can enter a judgment against you even though you are not present to defend yourself. A judgment is a court decision that you owe money. The judgment holder must follow legal procedures to try to collect on the judgment. The judgment holder may put a lien on your property, garnish your wages or bank account, or take personal property. However, the judgment holder cannot take certain property protected by law. This property is known as exempt property. Examples of exempt property include:

- ▶ Social Security, other government benefits, and pensions, which are exempt even when placed in a bank account;
- ▶ Household goods with a market value of up to \$3,000 per person. Market value is the cost a willing buyer would pay for a product “as is”;
- ▶ Up to two automobiles or bicycles with an aggregate market value of up to \$7,500 (\$12,500 for an elderly debtor);
- ▶ Clothing with a market value of up to \$2,000 per person;
- ▶ All prescribed health aids;
- ▶ All net wages if you earn less than a certain amount each week. If you earn more than a certain amount, a creditor cannot garnish more than 25 percent of your total net wages; and
- ▶ The first \$75,000 (\$105,000 for an elderly debtor) of equity in your house.

A creditor may try to take your property even though it is exempt. If this happens, you must file a claim of exemption with the court. The creditor or the court should mail the proper forms to you. This form will list your exempt property and stop the creditor from taking it. It doesn’t cost anything to file the claim of exemption, but you must act very quickly to protect your property.

11-3. Consumer Fraud

Charity Scams and Prevention

Seniors are the most generous contributors to charitable organizations. Unfortunately, there are many scams done in the name of charities, and older adults are often victims. Common scams include groups who use fake names of police, fire, disease and veterans organizations – causes that older adults are more likely to financially support. The Colorado Charitable Solicitations Act controls the activities of the persons who place the calls or mail the letters and the organizations they represent. Here are some of your rights:

- ▶ You have the right to ask if the solicitor is registered with the Secretary of State.
- ▶ If you make a donation in response to a telephone solicitation, the solicitor is required to give you a written confirmation of the expected donation. The confirmation should contain:
 - The name, address, and telephone number of the solicitor’s organization;
 - A disclosure that the donation is not tax deductible, if applicable;
 - A disclosure that the solicitor is a paid employee of a for-profit professional fundraiser;
 - The name, address, and phone number of the office from which the solicitation occurred; and
 - The name, address, and phone number of the charity associated with the solicitation.

You may cancel your donation if the solicitor has failed to provide any of the above information. You have three days after you get the written confirmation to cancel. The solicitor must refund your donation within 10 business days of your cancellation.

To ensure your charitable dollars are wisely spent:

- ▶ Make an annual charitable giving budget and list — and stick to it! Give once to those charities on your list, and disregard all other solicitations.
- ▶ Remember that many organizations intentionally use names that are similar to the names of well-known charities.
- ▶ Get proof that your deduction will be tax deductible, such as a letter from the U.S. Department of the Treasury stating that the organization qualifies under § 501(c)(3) of the Internal Revenue Code.
- ▶ Find out how much of your donation will go to the charity for programs and services and how much will be spent on fundraising. Contact the Better Business Bureau’s charity watchdog service at www.give.org or <http://denver.bbb.org>, or call (800) 222-4444 for a report.

Cyber Crimes

Crimes that occur over the internet are frequently associated with identity theft, and many of the same scams that come over the phone are also common online. The anonymity of the internet makes it especially easy for criminals to not just make a lot of money, but to leave emotional scars on their victims, and to get away with their crimes. An example of some of the bolder crimes include illegitimate dating sites or bogus suitors, online classified ads posted by disreputable brokers and sellers, and crooks who run ransomware scams on unprotected computers, as follows:

Online Dating Scams

As impossible as it is to believe that scammers are pretending to be in love with you for money, it's true, and victims lose hundreds of thousands of dollars. Online dating is a great way to meet new people, even the love of your life, but go into it with eyes wide open and learn the red flags.

You meet someone special on a dating website. Soon he or she wants to move off the dating site to e-mail or phone calls. He or she tells you he or she loves you, but lives far away — maybe for business, or because he or she is in the military.

Then he or she asks for money. He or she might say it's for a plane ticket to visit you, or emergency surgery, or something else urgent. The reasons never end.

Scammers, both male and female, make fake dating profiles, sometimes using photos of other people — even stolen pictures of real military personnel. They build relationships — some even fake wedding plans — before they disappear with your money. Make sure you don't send money. Never wire money, put money on a prepaid debit card, or send cash to an online love interest. You won't get it back. If you do have someone you feel could be the "one," do some checking to make sure you are talking to who you think you are:

- ▶ Run image searches of their profile photos at images.google.com or TinEye.com, and paste suspicious text into search engines to see if it's been used elsewhere.
- ▶ Pay attention if they have poor grammar or many misspelled words.
- ▶ Don't share personal information such as your address or date of birth.
- ▶ Be vigilant about users who ask you to leave the site and use personal e-mail addresses, and never send money — especially overseas.

Online Classified Ads

Free, online advertising sites are great ways of connecting buyers and sellers and promoting local services. However, victims report losing several thousands of dollars in scams involving rental properties, handyman services, unscrupulous caregivers, and bogus sellers and dealers. Although these sites have some protections in place to safeguard against abuse, it is ultimately up to the consumer to determine the authenticity of the seller, contractor, service, or product, before doing business. The following are some tips and precautions to take:

- ▶ Research the person, business, or service being offered. The Better Business Bureau or internet searches will often bring up interesting and helpful information on a person or business. Read any complaints that have been lodged, and why.
- ▶ Always verify the individual's credentials by asking for an ID and name of an official business.
- ▶ Do not select individuals advertising in-home care or services from online advertising sites. Instead, stick to professional companies that provide licensed and bonded caregivers.
- ▶ Make transactions in a public place if the buyer or seller is unknown to you.
- ▶ Do not do business with anyone who cannot be present to finalize a deal. Many reported complaints involve "out-of-country" solicitors who require businesses or consumers to wire money to a third party in exchange for the goods or services. To learn more about money transfer scams, go to www.westernunion.com/stopfraud.
- ▶ If possible, limit searches or advertising to a local geographical area.
- ▶ Know in advance what the market rate is for the product or service you are seeking, particularly if it is a home you would like to rent or buy. Any offer that is exceptionally above or below market rate for that area should raise suspicions.

Ransomware Scams

You are working on your computer when suddenly you are locked out. Common commands don't work, and then within seconds, a disturbing message pops up on your screen telling you that you have to pay to unlock your computer. The typical method of payment requested by the crook is usually a debit card.

Ransomware is a term used for a specific type of "malware," a particular virus introduced to your computer that allows crooks to search for files or photos you frequently use, then "encrypts," or locks them up. The following are some preventative steps consumers can take to avoid these scams, or to securely clean-up their computer.

- ▶ Be very careful about what you download on the internet. Viruses can unknowingly be introduced by clicking on links or opening attachments sent to you by strangers. Also be leery of downloading free, online documents. Only open e-mails from people you know.
- ▶ Store files, videos, pictures, and other important documents off your computer to protect from being exposed to malware.
- ▶ Always keep your computer updated with the latest security protections.
- ▶ If your computer or cell phone is infected, rather than paying the crook to decrypt the lock, take the machine to a reputable computer repair store and have them clean it up.

Extortion Scams

Also referred to as imposter scams, scammers will pretend to be someone they are not, and their method of extortion is to use scare tactics to get money out of their victims. Three very popular imposter scams are the IRS scam, the tech support scam, and the grandparent scam, and they work like this:

IRS Impersonation Scam

You get a call from someone who says she's from the IRS. She says that you owe back taxes. She threatens to sue you, arrest or deport you, or revoke your license if you don't pay right away. She tells you to put money on a prepaid debit card and give her the card numbers.

The caller may know some of your Social Security number. And your caller ID might show a Washington, D.C. area code. The real IRS won't ask you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card over the phone. And when the IRS first contacts you about unpaid taxes, they do it by mail, not by phone. And caller IDs can be faked.

- ▶ Here's what you can do: Stop. Don't wire money or pay with a prepaid debit card. Once you send it, the money is gone. If you have tax questions, go to irs.gov or call the IRS at (800) 829-1040.

Tech Support Scam

You get a call from someone who says he's a computer technician. He might say he's from a well-known company like Microsoft, or maybe your internet service provider. He tells you there are viruses or other malware on your computer. He says you'll have to give him remote access to your computer or buy new software to fix it. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything on your computer.

- ▶ Never give control of your computer or your credit card information to someone who calls you out of the blue.

Grandparent Scam

This scam is perpetrated over the phone by a caller pretending to be a grandchild in trouble who needs the grandparent to pay or wire money in order to avert their crisis at hand. The message is always urgent, and the victim must respond quickly before he or she has had a chance to think logically about the situation. In the typical scenario, the imposter grandchild is on vacation in another country and has been mugged or in an accident. Sometimes it's a grandchild in the military who has encountered some misfortune while stationed overseas. Victims may be contacted several times by the same caller, who will insist that more money is needed in order to make the problem go away.

- ▶ If you receive such a call, before doing anything, call your grandchild to verify the facts. Chances are your grandchild is safe and is in the United States. If you do not have your grandchild's phone number or are too frightened to take a risk, ask the caller to verify a fact known only to the family, such as the name of a beloved pet.
- ▶ If you have been scammed, once you realize what has happened, contact the wire service immediately and ask them to stop payment on your check. There is a remote possibility that you can recover your funds if the perpetrator on the other end has not picked up the cash.
- ▶ Report the scam to the Colorado Consumer Line at (800) 222-4444.
- ▶ Finally, be aware of what you and your family members post on social networking sites. Personal information about families is easy to obtain from these sites. Personal information can also be obtained through e-mail distribution lists and through obituaries, which routinely list the names of surviving family members and their relationships to the deceased.

Home Repairs and Improvement

Home repair scams are commonplace, and many seniors fall victim, especially if they live in a neighborhood where many older individuals reside. As is true with any product or service being offered, consumers need to know who they are dealing with before agreeing to do business. This is especially true with door-to-door solicitors. The following are important factors to consider before agreeing to any such service:

- ▶ Choose the persons you hire to do repairs and improvements on your home very carefully. Don't do business with anyone who comes to your door offering a bargain because he says he has materials left over from another job.
- ▶ Ask for references from previous customers and examples of the contractor's past work.
- ▶ On larger projects, get at least three written bids, and don't always choose the lowest bidder. Contact the Better Business Bureau for a report on any contractor you're considering.
- ▶ Never pay money in advance or make a final payment until you are satisfied with the work.
- ▶ Get the contractor's full name, address, phone number, and vehicle license plate number.
- ▶ Ask the contractor to show you proof that he is bonded, carries liability insurance, and covers his workers with workers' compensation insurance.
- ▶ Before deciding to hire someone to do your home repairs, get a detailed written estimate.
- ▶ It is important to agree upon a fee *before* work begins.

- ▶ Always get a written contract that specifies everything that was in the estimate, including all charges and costs, specific materials to be used, and the start and completion dates. You and the contractor both must sign the contract to make it binding. It is always a good idea to review the contents of this contract with your attorney before you sign.
- ▶ Make the financing of your job separate from the contracting for the work. Compare loans as carefully as you compare estimates from workers. Watch out for contractors that want to steer you to a particular lender, and never give the contractor a mortgage on your home.
- ▶ If you sign a loan for home repairs that involves a mortgage, you can cancel the loan within three business days from the day you signed the contract.
- ▶ The contractor may be entitled to what is known as a mechanics' lien. The law grants this special lien on your property for work performed there and not paid for. A mechanics' lien can also result in a forced sale of your home. Don't make a final payment to a home improvement contractor unless you've received a "lien waiver," which is a document showing that the contractor has paid his subcontractors and suppliers. These parties can place a mechanics' lien against your property as well if they aren't paid by the general contractor.

Sweepstakes and Prize Promotion Scams

Consumers are often enticed with a valuable prize or award to buy merchandise or services or to contribute to bogus charities. It isn't free if you have to pay a fee. If you have to buy a product like vitamins or light bulbs, pay a fee, or make a donation before you claim your award or receive your prize, you haven't won anything.

Sweepstakes companies prey on consumers' sense of greed and luck that they've won something for nothing. But sweepstakes companies are not in the business of giving away millions of dollars — they're in the business of making money.

Under Colorado's Sweepstakes and Contests Law, promoters are prohibited from engaging in any of the following:

- ▶ Falsely representing that you have won a prize;
- ▶ Falsely representing an item as a "prize" if it is given to all promotion recipients;
- ▶ Falsely representing that you have been specially selected or that you are in a select group of potential winners;
- ▶ Making false, deceptive, or misleading statements about your odds of winning or what you need to do to become eligible to win;
- ▶ Falsely representing that your envelope has been delivered by express or first-class mail;
- ▶ Displaying urgent messages on envelopes unless there is truly a limited time period for a sweepstakes entry and the true deadline is disclosed adjacent to the urgent message;

- ▶ Representing that sweepstakes entries accompanied by an order for products will be treated differently than entries without an order; and
- ▶ Creating a false impression of the solicitation's source, authorization, or approval.

The law requires a promoter to prominently disclose:

- ▶ A "No Purchase Necessary" message;
- ▶ The fact that the recipient has not yet won anything;
- ▶ The value of the prize;
- ▶ The odds of winning;
- ▶ The name of the promoter;
- ▶ The true deadline for entering the sweepstakes; and
- ▶ The official rules of the sweepstakes.

Law enforcement personnel recommend that you don't play sweepstakes, but if you do, remember:

- ▶ Don't pay to win. Buying products such as magazines doesn't increase your chances of winning a sweepstakes. You never have to pay to play when the contest is legitimate.
- ▶ No purchase is necessary to win. Prizes are free. If you have to pay before you can receive your prize, it's a purchase. It's against the law to require you to buy something to win a prize or participate in a sweepstakes or prize promotion.
- ▶ Be cautious of charities that use sweepstakes promotions. More of your donation is going to the promotion than to any charitable purpose.
- ▶ Keep your credit card and bank information to yourself. Never give your credit card number, bank account information, or Social Security number to anyone you don't know, especially if the reason is to verify your eligibility or to "deposit" winnings to your account.
- ▶ Lottery sweepstakes from foreign countries such as Canada and Australia are illegal. No foreign lotteries may be conducted in the United States.
- ▶ Participating in sweepstakes promotions is the best way for you to get on every junk mail list in the country. Selling your name to other direct mail marketers is a huge part of sweepstakes companies' business.

Telemarketing Scams

Coloradans lose millions of dollars a year to illegal telemarketers. A phone caller asks you to send money, and in return, you are promised that you will receive a much larger sum of money due to some unique opportunity. These callers are not salespeople just doing their job – they're criminals who will say anything to get your money. Do the following if you receive such a phone call:

- ▶ Be wary of a friendly voice or demeanor and someone who says they are a friend or relative but doesn't sound familiar.
- ▶ Never send money based on a promise given over the telephone from a stranger.
- ▶ If you suspect a scam, contact the police, your local district attorney's Office or the Better Business Bureau/Attorney General's Consumer Line at (800) 222-4444.
- ▶ For Canadian telemarketers, call Phone Busters at (888) 495-8501.
- ▶ It's hard to hang up on people, especially when the caller sounds so polite and friendly. But you wouldn't let a nice-looking stranger in your house or accept a ride from one, so handle telephone calls from strangers the same way.

Under the Colorado Telemarketing No-Call Law:

- ▶ Residential telephone customers can place their telephone numbers on a no-call list free of charge. (The law does not apply to business telephone customers.)
- ▶ You can sign up for the no-call list by calling (800) 309-7041 or registering online at www.coloradonocall.com.
- ▶ Commercial telemarketers may not call or send faxes to you at your home if you have placed your telephone number(s) on the no-call list, unless the telemarketer has an "established business relationship" with you.
- ▶ Calls by charities, political groups, and other non-commercial organizations are not subject to the Colorado No-Call Law.
- ▶ You have the right under the federal Telemarketing Sales Rules to tell companies with whom you have established business relationships to put you on their "Do Not Call" lists.
- ▶ Report offending telemarketers to the Attorney General or district attorney's office. You can also use the Colorado Consumer Protection Act to sue in small claims court if you are on the no-call list and get unwanted calls or fax transmissions from telemarketers.
- ▶ You can also add your home or cell phone numbers to the national Do Not Call list at www.donotcall.gov or by calling (888) 382-1222.

Federal Telemarketing Sales Rules

- ▶ Telemarketers can only call you between 8:00 a.m. and 9:00 p.m.
- ▶ Telemarketers must tell you it's a sales call, the name of the seller, and what they are selling before they make their pitch. If it's a prize promotion, they must tell you that no purchase or payment is necessary to enter or win.
- ▶ It's illegal for telemarketers to misrepresent any information; any facts about their goods or services; earnings potential, profitability, risk, or liquidity of an investment; or the nature of a prize in a prize promotion.

- ▶ Before you pay, telemarketers must tell you the total cost of the goods and any restrictions on getting or using them, or that a sale is final or non-refundable. In a prize promotion, they must tell you the odds of winning, that no purchase is necessary to win, and any restrictions or conditions of receiving the prize.
- ▶ It's illegal for a telemarketer to withdraw money from your checking account without your express, verifiable authorization.
- ▶ Telemarketers cannot lie to get you to pay, no matter how you pay.

11-4. Other Types of Financial Fraud

Health Insurance

- ▶ Do not purchase coverage you do not need or coverage that duplicates what you already have.
- ▶ Before buying or changing coverage, discuss your plans with someone you trust.
- ▶ The Colorado Division of Insurance operates a special counseling program for Medicare recipients and their families who need assistance in understanding Medicare benefits and coverage gaps, medical bills, and other insurance options, including long-term care insurance. For more information, call the Colorado Senior Health Insurance Assistance Program, (888) 696-7213 (for information in Spanish, call (866) 665-9668).

Hearing Aid Purchases

Unfortunately, scams involving hearing aid devices are prevalent. Some cautionary advice:

- ▶ Have an audiologist test your hearing before you decide to buy a hearing aid or replace an old one.
- ▶ Do not believe ads offering an effective hearing aid at a bargain price. You may get just what you pay for.
- ▶ Shop around and compare prices — for the fitting, adjusting, and servicing, as well as comparable aids.

By law, you may cancel an agreement to purchase a hearing aid within 30 days after receiving the hearing aid. You must return the hearing aid, and you are entitled to a full refund (except anything you may have paid for individualized ear molds). The law has other restrictions on the practices of hearing aid dealers. Talk to an attorney or call the Better Business Bureau/Attorney General Consumer Line at (800) 222-4444.

Predatory Lending

Predatory lending schemes are also on the rise. Predatory lending is the name given to an assortment of loans that take advantage of persons who borrow money. Predatory lenders target older homeowners by offering attractive-sounding loan offers that drain the value from their property. Some warning signs that you are a target for a predatory loan:

- ▶ You've fallen behind in your mortgage payments or you are already in foreclosure.
- ▶ You're getting phone calls and visits from companies offering to help you pay off your debts.
- ▶ A friend, advisor, or relative asks you to sign some forms without letting you read them.

To prevent predatory lending:

- ▶ Beware of companies who contact you in person or by fliers offering a foreclosure relief service.
- ▶ Don't sign any forms or papers without reading and understanding what you're signing. If you're uneasy or feeling pressured, get advice from a lawyer or other advisor.

If you're having trouble paying your mortgage, contact your bank or mortgage company and discuss potential payment plans.

Pre-Paid Funeral Plans

Be cautious when investigating a pre-paid funeral agreement. These contracts engage a specific funeral home (or cemetery) to deliver specific services at a set price upon a person's death. While it is a good idea to plan ahead so your family knows your wishes, some pre-paid plans are risky.

- ▶ Read the policy carefully and understand all of its terms before you invest in the plan.
- ▶ Know what happens if your wishes or circumstances change.
- ▶ Only work with reputable companies that have been in business for over five years.

Quit Claim Deeds

Quit claim deed fraud is another type of financial crime on the rise. A quit claim deed is a term used in property law to describe a document that allows one person to transfer any interest in a piece of property to another person. An example of a circumstance where a quit claim deed may be used legitimately is when one spouse (grantor) is disclaiming any interest in property that the other spouse (grantee) owns.

However, fraudulent transfers of property occur when a person convinces or coerces another into signing a quit claim deed that transfers ownership of property while not transferring the debt. Never sign a quit claim deed without getting the advice of an attorney. Once you have signed over property, it can be difficult or impossible to reverse.

11-5. Prevention Tools and Consumer Protections

Auto Repairs

These are your rights under the Colorado Motor Vehicle Repair Act:

- ▶ An auto repair facility must give a written estimate that includes the total cost, completion date, a statement of your right to have parts returned (except exchanged or warranty parts), and a statement on storage fees. You waive the right to an estimate if you sign a waiver, the vehicle is towed to the facility, or the vehicle is left before or after business hours. A customer must receive an estimate on any charge over \$100.
- ▶ If you have not been given a written estimate, the facility must call to get oral consent before the repairs can be done. The facility must record on the invoice or work order the date and time of the call, your name, the name of the employee making the call, and your phone number.
- ▶ The facility must give a written estimate that includes the cost of disassembly and reassembly and the costs of parts needed to replace those lost in disassembly. The facility must obtain oral consent before the repairs are completed. If more work causes an increase in the bill, the facility must obtain your consent before doing work. The oral consent must be recorded as described above.
- ▶ All parts and labor charges must be written clearly on the final bill. If the facility has not gotten approval, the final bill cannot be more than 10 percent or \$25 over the estimate, whichever is less.
- ▶ A facility may charge storage fees at the facility's discretion if the vehicle is not picked up within three business days of completion notification. Storage fees should be conspicuously printed on a separate authorization provided to the customer.

Contracts

Every word in a contract is important. Before signing any contract, read it in its entirety. If you do not understand any part of the document, ask for clarification and/or consult an attorney. Do not do business with anyone who refuses to give you a copy of the complete contract before you sign it.

If you and the other party come to an agreement about something that is not written in the document, you must put that agreement in writing. To make sure there are no misunderstandings, document all additions or deletions from the original document and all parties should initial or sign next to each change.

Most contracts are binding as soon as you and the other party sign. However, contracts from door-to-door sales and any contract that calls for placing a lien on your house can usually be cancelled within three days. Consumers have one day to cancel a contract that was solicited over the telephone.

Put all notices of cancellation in writing. It is recommended to send cancellation notices by certified or registered mail so you have documentation showing when you sent the notice, as well as receipt of the notice by the company. Also, never sign a contract with blank spaces that can be filled in later.

Do not sign a contract that takes away your legal rights unless you understand and agree to the consequences of such action. Keep copies of all contracts, receipts, payment records, and letters you send about the product or service.

Before you sign any type of sales or services contract, ask yourself these questions:

- ▶ Do I really want what I am paying for?
- ▶ Do I understand the contract I am about to sign?
- ▶ Do I know the total price, including interest and other charges, I will have to pay?
- ▶ Do I know how many payments I will have to make?
- ▶ Can I get the same thing somewhere else for a better price?
- ▶ Am I getting any guarantees on the product or for the services I am paying for?
(*Note: Get all guarantees in writing.*)
- ▶ Can I make the payments the contract requires?

Always remember that it will cost you far less to have an attorney review the contract before you sign than it will to have an attorney represent you in court because you made a deal that was unfair to you.

Security Freeze

If you don't anticipate opening any new credit accounts in the near future, you may want to consider placing a security freeze on your credit report. You have the option of requesting any consumer reporting agency (credit bureau) to place a security freeze on your credit report. A freeze means your file can't be shared with potential creditors. You must request separate security freezes for each of the three credit reporting agencies, in writing via certified mail. Please see Exhibit 11A at the end of this chapter for a sample letter you may use to request a security freeze.

Equifax Security Freeze

www.equifax.com; click on "Credit Report Assistance," then "Place a Security Freeze on Reports."

Experian Security Freeze

www.experian.com/consumer/security_freeze.html

TransUnion Security Freeze

www.transunion.com; click on "Credit Report Assistance," then "Credit Freeze."

Consumer reporting agencies must place a security freeze on your credit report within five business days after receiving your written request and must send you written confirmation of the security freeze within 10 business days. They will provide you with a unique personal identification number or password for you to use in providing later authorization for the release of information from your credit report.

If you want potential creditors to be able to access information on your credit report, you must request that the freeze be temporarily lifted and provide the following information:

- ▶ Proper identification;
- ▶ The unique personal identification number and password provided by the consumer reporting agency; and
- ▶ The proper information regarding the third party who is to receive the credit report or the time period that the report shall be available.

The consumer reporting agency must remove a security freeze within three business days of receiving a request. The initial security freeze is free of charge; however, the temporary or permanent removal of the freeze, as well as the reinitiating of a freeze, will cost up to, but no more than, \$12 per action.

11-6. Resources

The following are excellent resources for information on your rights as a consumer or to report complaints:

For issues related to fraud:

24-Hour Identity Theft Hotline

Colorado Bureau of Investigation
ID Theft/Fraud Investigation Unit

690 Kipling St., Ste. 4000

Lakewood, CO 80215

(855) 443-3489

(303) 239-4211

www.colorado.gov/cbi, click on "Sections," then "Investigations," then "Identity Theft"

Colorado Consumer Line

AARP ElderWatch, Better Business Bureau, Attorney General's Office

(800) 222-4444 (toll-free)

(303) 222-4444 (metro Denver)

www.aarpelderwatch.org

www.bbb.org

www.coloradoattorneygeneral.gov

Attorney General's Office Consumer Protection Section

For questions about credit and debt issues

(800) 222-4444

First Judicial District (Jefferson and Gilpin counties)

District Attorney's Office, Consumer Fraud: (303) 271-6931

Second Judicial District (Denver County)

District Attorney's Office, Consumer Fraud Hotline: (720) 913-9179

Fourth Judicial District (El Paso and Teller counties)

District Attorney's Office, Consumer Line: (719) 520-6000

Seventeenth Judicial District (Adams and Broomfield counties)

District Attorney's Office: (303) 659-7720

Eighteenth Judicial District (Arapahoe, Douglas, Elbert, and Lincoln counties)

District Attorney's Office, Consumer Protection Line: (720) 874-8547

Twentieth Judicial District (Boulder County)

District Attorney's Office, Consumer Protection Line: (303) 441-3700

Twenty-First Judicial District (Mesa County)

District Attorney's Office, Consumer Protection Unit: (970) 244-1730

For Medicare insurance issues:

Colorado Senior Health Insurance Assistance Program

(888) 696-7213

www.dora.colorado.gov/insurance, click on "Senior Healthcare/Medicare"

For financial planning:

Colorado Division of Securities

(303) 894-2320

To request a free copy of your credit report once a year from the three major credit reporting companies:

(877) 322-8228

www.annualcreditreport.com

Credit reporting agencies:

Equifax
(888) 766-0008
www.equifax.com

TransUnion
(800) 888-4213
www.transunion.com

Experian
(888) 397-3742
www.experian.com

For home repairs and improvements:

Contact your city or county building department to check on building permits and license status of contractors.

To “opt out” of credit card solicitations:

(888) 5-OPTOUT (567-8688)
www.optoutprescreen.com

No-call lists:

In Colorado: (800) 309-7041 or www.coloradonocall.com
Nationally: (888) 382-1222 or www.donotcall.gov

Area Agencies on Aging:

Logan, Morgan, Phillips, Sedgwick, Washington, and Yuma counties:

Region 1
Northeastern Colorado Association of Local Governments
Northeastern Region
Fort Morgan
(970) 867-9409

Larimer County:

Region 2A
Larimer County Office on Aging
Northeastern Region
Fort Collins
(970) 498-7750

Weld County:

Region 2B
Weld County Area Agency on Aging
Northeastern Region
Greeley
(970) 346-6950

Adams, Arapahoe, Broomfield, Clear Creek, Denver, Douglas, Gilpin, and Jefferson counties:

Region 3A
Denver Regional Council of Governments
Northeastern Region
Denver
(303) 455-1000

Boulder County:

Region 3B
Boulder County Area Agency on Aging
Northeastern Region
Boulder
(303) 441-3570

Park, El Paso, and Teller counties:

Region 4
PPAGC Area Agency on Aging
Southern Region
Colorado Springs
(719) 471-2096

Cheyenne, Elbert, Kit Carson, and Lincoln counties:

Region 5
East Central Council of Governments
Northeastern Region
Stratton
(719) 348-5562, ext. 5

Baca, Bent, Crowley, Kiowa, Otero, and Prowers counties:

Region 6
Lower Arkansas Valley Area Agency on Aging
Southern Region
La Junta
(719) 383-3166

Pueblo County:

Region 7
Pueblo Area Agency on Aging
Southern Region
Pueblo
(719) 583-6120

Alamosa, Conejos, Costilla, Mineral, Rio Grande, and Saguache counties:

Region 8
South-Central Colorado Seniors, Inc.
Southern Region
Alamosa
(719) 589-4511

Archuleta, Dolores, La Plata, Montezuma, and San Juan counties:

Region 9
San Juan Basin Area Agency on Aging
Western Region
Pagosa Springs
(970) 264-0501

Delta, Gunnison, Hinsdale, Montrose, Ouray, and San Miguel counties:

Region 10
League for Economic Assistance & Planning
Western Region
Montrose
(970) 249-2436

Garfield, Mesa, Moffat, Rio Blanco, and Routt counties:

Region 11
Associated Governments of Northwest Colorado
Western Region
Grand Junction
(970) 248-2717

Eagle, Grand, Jackson, Pitkin, and Summit counties:

Region 12
Northwest Colorado Council of Governments
Alpine Area Agency on Aging
Western Region
Silverthorne
(970) 468-0295

Chaffee, Custer, Fremont, and Lake counties:

Region 13
Upper Arkansas AAA
Southern Region
Salida
(719) 539-3341

Huerfano and Las Animas counties:

Region 14
Huerfano/Las Animas Area Council of Governments
South Central Council of Governments AAA
Southern Region
Trinidad
(719) 845-1133

Legal Assistance Developer for the Elderly

Disability Law Colorado

455 Sherman St., Ste. 130
Denver, CO 80203
(303) 722-0300
<http://disabilitylawco.org>

Colorado Crime Victims Compensation Programs

First Judicial District

District Attorney's Office
500 Jefferson County Pkwy.
Golden, CO 80401
(303) 271-6846

Sixth Judicial District

1060 Main Ave.
P.O. Drawer 3455
Durango, CO 81302
(970) 247-8850

Second Judicial District

201 W. Colfax, Dept. 801
Denver, CO 80202
(720) 913-9253

Seventh Judicial District

1140 N. Grand Ave., Ste. 200
Montrose, CO 81401
(970) 252-4266

Third Judicial District

200 E. 1st St., Ste. 302
Trinidad, CO 81082
(719) 846-9224, ext. 108

Eighth Judicial District

201 La Porte, Ste. 200
Fort Collins, CO 80521
(970) 498-7290

Fourth Judicial District

105 E. Vermijo, Ste. 111
Colorado Springs, CO 80903
(719) 520-6915

Ninth Judicial District

109 8th St., Ste. 308
Glenwood Springs, CO 81601
(970) 384-3517

Fifth Judicial District

P.O. Box 295
Eagle, CO 81631
(970) 337-3704

Tenth Judicial District

701 Court St.
Pueblo, CO 81003
(719) 583-6092

Eleventh Judicial District

136 Justice Center Rd., Rm. 203
Cañon City, CO 81212
(719) 269-0170

Twelfth Judicial District

426 San Juan Ave.
Alamosa, CO 81101
(719) 589-3691

Thirteenth Judicial District

400 Warner St.
Fort Morgan, CO 80701
(970) 542-3473

Fourteenth Judicial District

221 W. Victory Way, Ste. 302
Craig, CO 81625
(970) 824-9143

Fifteenth Judicial District

110 E. Oak St.
Lamar, CO 81052
(719) 336-7446

Sixteenth Judicial District

323 Santa Fe, Ste. 201
La Junta, CO 81050
(719) 384-8786

Seventeenth Judicial District

1000 Judicial Center Dr., Ste. 100
Brighton, CO 80601
(303) 835-5562

Eighteenth Judicial District

6450 S. Revere Pkwy.
Centennial, CO 80111
(720) 874-8607

Nineteenth Judicial District

P.O. Box 1167
Greeley, CO 80632
(970) 356-4010, ext. 4748

Twentieth Judicial District

Boulder County Courts Building
1035 Kimbark St.
Longmont, CO 80501
(303) 682-6801

Twenty-First Judicial District

P.O. Box 20,000-5031
Grand Junction, CO 81502
(970) 244-1737

Twenty-Second Judicial District

103 N. Chestnut St.
Cortez, CO 81321
(970) 564-2755

Elder Abuse:

Call 911 or your local police department.

Adult Protection

Call your county Department of Social Services. You may find a list of contact information for these offices at www.colorado.gov/cdhs; click on "Services by County."

AARP ElderWatch

Through the Colorado Consumer Line: (800) 222-4444, option 2, for referrals and assistance information.

Metro Denver: (303) 222-4444

www.aarpelderwatch.org

First Judicial District (Jefferson and Gilpin counties)

District Attorney's Office: (303) 271-6931

Second Judicial District (Denver County)

District Attorney's Office: (720) 913-9179

Seventeenth Judicial District (Adams and Broomfield counties)

District Attorney's Office: (303) 659-7720

Eighteenth Judicial District (Arapahoe, Douglas, Elbert, and Lincoln counties)

District Attorney's Office: (720) 874-8547

Twentieth Judicial District (Boulder County)

District Attorney's Office: (303) 441-3700

*Based on a chapter originally written by Lisa Curtis, Office of the District Attorney, Second Judicial District, and later updated by Janice L. Friddle, AARP ElderWatch; Sally B. Hume, Esq., AARP Financial Security; and Robin Fudge Finegan, M.A., M.N.M., FEMA Region VIII.

Exhibit 11A.
Sample Letter for Credit Freeze Request

[Date]

Dear [Agency Name]:

Please place a security freeze on my credit file.

My name is _____.
(one name only, spouse must fill out separate request)

My former name was (if applies) _____.

My current address is _____.

My address has changed in the past five years. My former address
was _____.

My Social Security number is _____.

My date of birth is _____.

I have included photocopies of a government issued identity card AND proof
of residence such as a utility bill or phone bill.

Yours Truly,

Signature _____

Send by Certified Mail Only