Chapter 24

Arm Yourself with Consumer Protection Information

Mark Fetterhoff
AARP ElderWatch

SYNOPSIS

24-1. Recognize — Refuse — Report

Financial exploitation cannot be completely prevented, but AARP ElderWatch strives 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, hang up the phone, or disconnect online; (4) know how to report fraud to the appropriate agencies; and most importantly, (5) empower yourself. We value educating older Coloradans because we know that education is one of the most important factors in preventing consumer fraud.

24-2. Identity Theft and Data Breaches

Identity Theft

Identity theft is one of the most common types of fraud reported in Colorado. 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; 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 can spend months or even years trying to regain their financial health.

Ways to protect against identity theft:

- Don't leave your purse or wallet unattended in public areas.
- Regularly audit your wallet or purse for extra information that might be valuable for criminals, but not something needed on a daily basis. This includes your Social Security card. Take it out of your wallet today!
- 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 and ask you to "confirm" your SSN or other information.
- Shred pre-approved credit card offers and any papers that have your personal information using a cross-cut shredder.
- Keep a record and/or copies of your credit card numbers and their 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.
- To avoid the risk of convenience checks that come with credit card offers being lost or stolen, "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 names or numbers or commonly chosen words (*e.g.*, Password123, 123456, a pet's name, etc.) as passwords or PINs. Consider *two-factor authentication* as a second form of account verification if you can receive a PIN confirmation on your cell phone.
- Consider using a passphrase rather than a password, something easy to remember but also hard to guess with an increased amount of characters. Change passwords frequently if you do a lot of business over the internet — see "Cyber Crimes" under section 24.3, "Consumer Fraud."
- Utilize biometric options like fingerprints and facial recognition for accessing devices like phones, computers, and tablets, if available.
- Whether checking paper bank statements or banking online, be sure to dispute discrepancies with your credit card statements as soon as possible. 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.
- Request a free copy of your credit report from the three major credit reporting bureaus: (877) 322-8228 or online at www.annualcreditreport.com.

If you think your identity has been stolen:

- Visit the Federal Trade Commission's Identity Theft website www.identitytheft.gov to file a report and create a personalized action plan.
- Considering filing a report with local law enforcement, especially if you believe your identity was stolen by someone in your community.
- Contact the fraud departments at one of the three major credit reporting bureaus and place a fraud alert on your credit report: Equifax, (800) 685-1111; 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.
- For additional specialized assistance contact the Colorado Bureau of Investigation Victim's Assistance Hotline (855) 443-3489.

Data Breaches

Data breaches are defined as the unauthorized (criminal) hacking of commercial or governmental networks for the purpose of stealing sensitive information on a consumer or entity. Like identity theft, this stolen information can be used by criminals for financial gain. However, unlike traditional forms of identity theft, consumers have no way of preventing a data breach from occurring, or their personal information from possibly getting into the hands of a thief. Also remember, just because your information may have been uncovered **does not** mean you are an actual victim of identity theft at that time. The following precautions should be undertaken to keep any financial information that may have been exposed from being used by an identity thief or crime ring:

- Follow the instructions given on the website of the business or entity whose network has been breached. Some companies may offer free identity theft monitoring services for a limited period of time, or other reparations. Note that credit reporting agencies must offer free electronic credit monitoring to all active-duty military.
- Consider placing a freeze on your credit with each of the three credit reporting bureaus (Equifax, (800) 685-1111; Experian, (888) 397-3742; TransUnion, (888) 909-8872). A freeze will stop creditors or thieves from accessing your report. Freezing and un-freezing your credit it free.
- Run a credit report at least annually and review it thoroughly to see if any accounts have been opened in your name and/or without your approval. This is one of the most effective means of discovering if you are a victim of identity theft. A copy of your credit report can be obtained at (877) 322-8228 or online at www.annualcreditreport.com.

If you discover your personal information has been used to impersonate you:

- File a police report.
- Place a fraud alert on your credit report by notifying one of the three credit reporting bureaus and your financial institutions to discuss options, such as placing a fraud alert on accounts or closing your accounts and opening up new ones. An initial fraud alert will last for one year. It will be free, and identity theft victims can get an extended fraud alert for seven years. Visit www.identitytheft.gov for detailed instructions, websites, and phone numbers.
- Follow the steps recommended under "Identity Theft," above.

24-3. Consumer Fraud

Charity Scams and Prevention

Older adults are often 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:

- Visit www.checkthecharity.com to ensure the charity you are giving to is registered to solicit donations with the Colorado Secretary of State's Office.
- Make an annual charitable giving plan — and stick to it! Give only 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 to confuse donors.
- Get proof that your donation 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.
- Do your research by visiting charity watchdog sites like www.charitynavigator.org or www.give.org.

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. Some examples of the bolder crimes include illegitimate dating sites or bogus suitors and online classified ads posted by disreputable brokers and sellers, 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 can be a successful way to meet new people — even the love of your life — but go into it with eyes wide open and learn to recognize the following red flags:

- You meet someone on a dating website or someone messages you on social media. Soon he or she wants to move the conversation to another platform like text messages, WhatsApp or Google Hangouts.
- The person gets very serious, very quickly, even professing their love and that although you both live far away — perhaps due to work or military duty — someday you both will be together.
- He or she asks for money on the pretense of covering plane fare to visit you, or for emergency surgery, or something else very urgent. There are always a host of reasons.
- Recently, romance scams have also been tied to investment in cryptocurrency. It is not uncommon for a romantic interest to pose as an "expert" in cryptocurrency, who could make a lot of money for you if provided him or her with cash to invest. The second the person you are speaking with promises to double your money, it is time to disconnect.

Scammers, both male and female, use 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 or goods to anyone you haven't met before. Never wire money, purchase a gift card, send cash, or buy goods (computers, phones, etc.) for 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 the person 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 or financial information with anyone.
- Be vigilant about users who ask you to leave the site and communicate elsewhere.
- Trust your gut! If something feels a little off or "too good to be true," it is probably a scam. It's time to move on and report the criminal to the platform you met them on.

Online Marketplace Sales

Marketplace sites and apps like Craigslist, Facebook Marketplace, OfferUp, and Nextdoor can be a great way to connect buyers and sellers and promote local services. However, criminals are also lurking on these platforms. Victims report losing thousands of dollars in scams involving rental properties, handyman services, auto sales, 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 product or service being offered. Understand what the market value of the product or service is before inquiring. A product or service outside of market value should be considered a "red flag" of a potential scam.
- 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 buyer or sellers who are not local. Solicitors who require businesses or consumers to wire money or pay via a peer-to-peer payment app (*e.g.*, Vemno, Zelle, Cash App, etc.) to a third party in exchange for the goods or services are likely a scam.

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 government imposter scam, the tech support scam, and the grandparent scam, and they work like this:

Government Impersonation Scam

You get a call from someone who says she's from the IRS or Social Security Administration. She says that you owe back taxes or there is something wrong with your benefits. 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 gift 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. Keep in mind that caller IDs are often faked — a ploy that is known as "spoofing" — to scare you into picking up the receiver. To prevent being taken in this scam:

- Large government entities like the IRS and Social Security will not call you. Never answer the phone. Instead, let the message roll into voicemail and delete it from there.
- Never send money, even if you believe it's a legitimate call. Don't wire money or pay with a prepaid gift card, because once you send it, the money is gone.

Tech Support/Computer Virus Scams

One of the most common scams reported in Colorado are tech support or computer virus scams. Computer users receive an unsolicited contact alerting them that there is an issue with their computer, tablet, cellphone, or other device that connects to the internet. Scammers often pose as someone who works at a well-known computer company like Microsoft, Apple, or Hewlett Packard to try to gain the trust of their victims. Recently, these criminals also have started to pose as workers from large computer virus protection software companies like Norton or McAfee. They contact victims over the phone, through a pop-up on a computer, or by creating a fake consumer support website. The following are some preventative steps consumers can take to avoid these types of scams:

- Hang up on unsolicited callers who claim to be with a computer company. Never let any unsolicited caller or unknown entity remotely access your computer or device.
- Always keep your computer updated with the latest security protections, including antivirus software and system updates to your device.
- If someone accesses your device and you believe they have bad intentions, shut it down, unplug it, or both to stop the connection with the scammer.
- If your computer or cell phone is infected, take the machine to a reputable computer repair store and have them clean it up.
- 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 emails from people you know.

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 grandparent must respond quickly before he or she has had a chance to think logically about the situation. In the typical scenario, the grandchild is in another country and has been mugged or in an accident. 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 sent money to the criminal, once you realize what has happened, contact the wire service or payment method immediately and ask them to stop payment. There is a remote possibility that you can recover your funds if the perpetrator on the other end has not picked up the cash.
- 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 email distribution lists and through obituaries, which routinely list the names of surviving family members and their relationships to the deceased.

- This type of scam can happen with other familial relationships as well. Nieces and nephews, and even spouses. Stay calm, take time to think, and check with others before taking action.

Home Repair and Improvement Scams

Home repair scams are commonplace and take a few forms, either a fly-by-night operation that never does/partially does a job or is often a disagreement with a contractor. 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 or she says he or she 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 if it means compromising the extent of, or quality of the work you want done.
- Contact the Better Business Bureau (www.bbb.org) or other consumer review sites to find a business, and then review that company's rating and report.
- Never pay 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 the business is bonded, carries liability insurance, covers workers with workers' compensation insurance, and is licensed to do business in your municipality. Contractors cannot pull a permit unless they are licensed. Verify this with your local building department before deciding on a contractor.
- 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. On high ticket items, it is always a good idea to review the contents of this contract with your attorney before you sign.
- 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 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. The number one "red flag" of a sweepstakes scam is that you have to pay money to receive money. No matter what the excuse of the criminal is, even if they are using a common sweepstakes name like Publisher's Clearing House, never provide anyone with money to claim a prize.

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.

Unwanted Calls

Unwanted calls have dramatically increased in recent years. Solicitation calls are channeled through the internet via Voice-over Internet Protocol (VoIP), making it possible for telemarketers and criminals to place vast numbers of calls through the phone network at a fraction of the cost. Dishonest businesses and criminals were quick to jump on board.

Traditional landline (analog) phone users are the most vulnerable to unwanted calls, compared to those who have VoIP phone systems, due to their outdated technology, which lacks the ability to effectively block unwanted calls. Do the following if you receive such a phone call:

- Let the call roll over into voicemail if you don't recognize the number or information on caller ID, especially if you are using a landline phone. Use voicemail to screen out the call.
- If using a landline phone, check with your phone carrier on how to block unwanted calls.
- VoIP and cell phone users can block unwanted calls by signing up for Nomorobo at www.nomorobo.com. Nomorobo is a service that runs through internet-connected phone systems. It stops unwanted calls by filtering out numbers known to be associated with scams.
- Unwanted calls that come through cellular phones can be screened out through downloadable apps developed for just this purpose. To avoid possible malware infection, make certain the app you select comes from a reliable source, such as an official app store.
- Never send money based on a promise given over the telephone from a stranger.

Note: Phone carriers, working in partnership with the Federal Communications Commission (FCC) and other regulatory and legislative bodies, have rolled out an initiative that helps to curb the amount of robocalls. This initiative, an acronym referred to as SHAKEN/STIR, allows phone companies to "opt out" of sending suspicious, unverifiable robocalls on to consumers. Additionally, several phone companies are now offering free call-blocking services to their customers. For more information on call-blocking services, or on the SHAKEN/STIR initiative, contact your phone company.

24-4. 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 State Health Insurance Assistance Program, (888) 696-7213 (for information in Spanish, call (866) 665-9668).

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.

24-5. 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.

Credit Repair

Television 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

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

- TransUnion
  To order a credit report by:
  Phone, (888) 909-8872
  Internet, www.transunion.com

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.

No-Call Registry

Residential telephone customers can place their telephone numbers on a no-call list free of charge. However, 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. The following applies under the No-Call Law:

- 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. 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 number to the national Do Not Call list at www.donotcall.gov or by calling (888) 382-1222.

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 at:

- **Equifax Security Freeze**
  www.equifax.com; click on "Credit Report Help," then "Place a Security Freeze."
- **Experian Security Freeze**
  www.experian.com/freeze/center.html
- **TransUnion Security Freeze**
  www.transunion.com; click on "Services," then "Freeze Credit Report."

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.

24-6. More Information

For more information and excellent resources for information on your rights as a consumer or to report complaints see Appendix A: Resources, Chapter 24.