Chapter 23
Protecting Yourself from Crime

Stephen C. Fauver, J.D., M.S., C.F.E.
18th Judicial District Attorney's Office

SYNOPSIS

23-1. Protection Outside Your Home

Protection outside of our homes starts with the need for all of us to do a little planning before we leave, to be aware of distractions that may lead to us being unfairly surprised, and to recognize that we may be an intentional or random target of crime.

- ✦ We all face an increased risk of violent encounters with other drivers. Honking, gesturing, yelling, and aggressive driving can lead to violence. If faced with this situation, do not engage or participate in the encounter. Note what you can of the car and driver's description but do not chase or follow. If you cannot make a hands-free emergency call, drive to a police station or public area and call 911.
- ✦ Walk with confidence and remain aware of your surroundings. Do not let your cell phone distract you so that you become unaware of possible dangers. Your unlocked cellphone is an open wallet; do not give it to others or volunteer to make their calls.
- ✦ If you are going out alone, let someone know your plans. When out alone, keep a whistle or personal body alarm handy and hold your keys in your hand while walking. Learn the emergency call features of your cellphone and how to disable and wipe it if it is stolen.
- ✦ Park in well-lit areas as close as possible to the door of your destination. Do not be embarrassed to ask someone to walk you to your car.
- ✦ Lock your car doors at all times and keep windows rolled up when possible. Do not use the remote control to open your car door until you are next to the car.
- ✦ Look behind you, under, around, and inside your car before getting in it. Be aware of your surroundings before getting out of your car, including inside your garage.
- ✦ Keep your wallet or purse where thieves cannot reach it. A close-fitting pouch is more secure than a purse. Your cellphone is essentially a wallet — Protect it!

- Hold your purse firmly and do not leave it outside your line of sight or unattended on a counter, grocery cart, or car seat. If your window is down, thieves can grab your bags.
- Only carry the cards and limited cash you know you will need that day and never carry your Social Security card. Never carry a large sum of money.
- Never write your PIN number on your ATM or Electronic Banking Transfer cards, or anywhere in your wallet. Do not keep a written list of passwords in your wallet, either.
- Avoid ATM machines in deserted areas, including drive-up locations. Instead, use ATMs in stores, bank lobbies, or well-lit areas. If people nearby or the situation causes you any concern, leave immediately. Immediately secure your money before walking away.
- Keep a list of your credit cards somewhere other than your wallet to make it easier to report a loss. Use a copy machine or scanner to copy the front and back of all cards and keep the copies safe. Report any loss immediately.
- Avoid waiting at deserted bus stops. Consider walking to the next bus stop where others may be waiting. Also, consider taking a taxi or ride-share service (Uber/Lyft/other) and ask the driver to wait until you are inside your home.
- If you are riding the bus, be aware of anyone who might be staring at you. Tell the bus driver if you are concerned about your safety. You can prevent trouble by anticipating it.
- If someone grabs your purse or bag, do not put yourself at risk by resisting. If you try to resist, you may be injured. Other options are to sit down to avoid being knocked down, make noise, whistle, or call for help. In any case, tell the police as soon as possible.
- Elders are constant targets for fraudsters who approach them in public with fake promises of help or services. Confidence artists will approach you with promises that they can repair damage to your car or provide you with other services. They may claim they have done work that you are now obligated to pay them for. Practice your response and be firm: "I am not in a position to help you; I do not want you to do anything to my (car, home, yard); I did not give you permission to do anything to my (car, home, yard) so I will not pay you anything; I will call the police if you do not leave me alone." Do not pay these scammers, do not be embarrassed to call for police assistance, and DO NOT TAKE THEM TO YOUR HOME for any reason.
- Always remember—your life and well-being are more important than your belongings.

Victims' compensation programs help victims of violent crimes with medical and other bills but will not replace stolen items or cash. If the police take a report, assistance is available even if no criminal case is filed. For more information or an application form, contact your local police department or district attorney's office.

23-2. Protection at Home

Protection at home focuses on efforts to make your home less attractive to burglars and fraudsters. This involves adding security features to deter burglars and to make it more difficult for them to enter your home, adding cameras and other technology to help notify you of break-ins and identify criminals, efforts you should take to document what may be stolen for the police and insurance companies, and precautions you should take to limit access by strangers.

- Do not list your first name on your mailbox.

- Consider installing a doorbell camera and other cameras covering other doors and windows, and save video to cloud storage. Video may be viewed on a computer, tablet, cellphone, or device such as an Amazon Echo, Google Home, or other device.
- Consider installing a security system including alarm, door/window sensors, movement sensors, and cameras. Some systems can be monitored by the renter or homeowner alone or in conjunction with a monitoring company that will contact the police. Lock your doors and windows whether you are at home or away and remember to keep your screen or storm door locked. Keep burglar alarms armed when home or in the yard to keep thieves from sneaking inside.
- When at home, keep your shades pulled at night and when you are undressing. Be cautious as to who knows you are alone. If someone is outside your window, call the police.
- Keep outside lights near doors and large windows turned on. Strong outside lighting helps prevent burglaries. Consider adding additional outdoor lighting.
- Keep your garage door closed and lock the inside door to your garage. Check both doors at night to ensure both are closed and locked. Do not keep valuables in your car, even if it is in a garage. Newer garage door systems can be scheduled to close automatically.
- Use deadbolt locks that require a key inside and outside (but keep your key in the inside of the door in case of a fire). Consider having a contractor strengthen door frames and doors to make it more difficult to force entry.
- Consider replacing the glass in or next to your door with Plexiglas or Lexan or covering it with a decorative iron grill.
- Inside locks should secure all windows, except emergency exits. Place a broomstick or pole in the track of sliding doors or windows so they cannot be forced open by a burglar.
- Trim shrubs and bushes hiding doors and windows because they make excellent cover for burglars. Notify your landlord of all safety risks and concerns.
- Never leave a firearm unsecured or unlocked. You must report any stolen firearms to the police.
- Your front door is the gateway to your personal castle — GUARD IT! When someone knocks at your door, first check to see who it is and do not open your door to a stranger. Fraudsters often wear fake uniforms and safety vests. Your personal safety is more important than someone thinking you are rude. Do not hesitate to ask the person to come back later, when you can have another person with you. Check identification and confirm references before you let anyone into your house and confirm directly with the landlord before allowing service people inside. It is okay to be suspicious, especially when more than one person wants to come inside; it is a common scheme for one person to keep you busy while the second person steals from you. Your home — your rules, so it is okay to demand that no one is permitted to be unescorted in your home.
- Do not keep large amounts of money in your home. Given enough time, burglars will find any hidden valuables and can break into any residential safe. Be sure valuables are insured with up-to-date appraisals and use a bank safe deposit box.
- Call your local police department for a home security and personal safety review of your home. Call your local fire department for help designing a fire safety plan. Always have fire extinguishers and fire blankets available. Keep titles, receipts, appraisals, and other important documents in a fire-rated safe or safe deposit box.

- If something is stolen from your home, you will need to prove to the police and others that you owned it and that it had a particular value if you want to get it back or get compensation for it. Mark your valuables with an identification number (not your SSN) or name. Take detailed photographs of all jewelry, artwork, firearms, electronics, and other valuables, including serial numbers, and keep copies of the photos in a digital cloud account, in a safe deposit box, or with your insurance agent. Be prepared when the insurance company or police ask, "Where is your purchase receipt; Where is your current appraisal by an expert?"
- Do not hide valuables in locations you may forget or places you do not share with others. Countless family heirlooms and valuables have been lost forever when the elder forgets where they were hidden, the family can't find them or a stranger finds them and keeps them.
- When planning to be away from home, never hide a door key. A neighbor, friend or family member can keep an extra key for you. Protect any digital access key codes. Create a temporary code for others and delete it when you return.
- Turn on some inside lights when you are away. Use timers and remote access to vary the lights you turn on and off. Put remote cameras inside your home, so you can check on the condition of your home. Include a water sensor alarm near the washer and water heater. Check the weather report before you leave; it is better to keep the house warm or cool rather than risk pipes freezing or damage from excessive heat.
- When you plan to be away from home for a long time, tell the police. Ask a friend or family member to check inside and outside your home each day, turn on different lights, pick up mail and newspapers, mow the grass, and set out the trash, if necessary. Do not forget to request a hold on mail delivery.

23-3. Protection on the Computer and Telephone

No one wants to be tricked into giving money to liars and thieves. Unfortunately, we are being constantly bombarded with false communications designed to take our money. We must be skeptical of every letter, phone call, text message, and email we receive. Remember, we must always assume these communications may be fraudulent until we are convinced the sender or caller is not an artificial intelligence bot or fraudster. Caller IDs, phone numbers, and email addresses, including those of police and government officials, are being "spoofed" to appear legitimate when they are not. Criminals continue to use regular mail and telephone calls to target victims. They are increasingly using text messages more than email and QR codes.

- The criminals that are targeting us with scams and fraud schemes are often working for countries such as North Korea, China, Russia, or Iran, or they are part of trans-national organized crime rings. These are typically sophisticated operations involving many people. It is best to avoid or quickly disengage from any attempts to defraud you. Any enjoyment you may get from messing with a fraudster is not worth the risk you face if they decide to retaliate against you using their cybercrime resources.
- Telecommunication fraud schemes (using internet, video, telephone, text messaging, and emails) are increasingly being supported by the use of artificial intelligence to create deepfake videos and audio to impersonate people, as well as improve the appearance and grammar in fake text messages and emails. Slow down and take extra steps to verify any communication.

- Romance and other relationship scams are emotionally, if not financially, devastating to the victim. Once a victim begins to believe the lies he or she is told, it is very difficult for them to recognize and accept that they are the victim of a crime. If you are involved in a long-distance relationship where you have never had an in-person meeting, please be cautious and share your experiences with trusted family and friends. Trust but verify.
- How can we protect ourselves? First, understand that we are not bad people if we do not trust strangers and require that others earn our trust. Unfortunately, we must all be skeptical of every unsolicited communication.
- Second, do the best we can to recognize when we are the target of a fraud scheme by knowing how they work. Look for notices of new schemes and share them with others.
- Third, be unafraid to stop whatever we are doing to ask others to apply their knowledge and experience to our situation. Do not be embarrassed to HANG UP THE PHONE to give yourself time to think and consult with others before you take any action.
- The fraudsters that perpetrate these types of schemes are experts in human psychology and practiced confidence artists that have years of experience and actually use scripts with multiple people playing different roles to convince victims that giving the criminals personal and financial information and money is a good idea at the time.
- Common elements include a "hook" to get your attention, an "emergency" to keep you from applying your reason and common sense, and a "send" where the victim is asked to give something to another. Positive hooks tell you that you won or earned something good, that you have an opportunity to help others by donating money, that you have inherited money, or that the person on the other side of the communication thinks you are special and they want to have a relationship with you. A negative hook is one where you are: threatened with legal action or arrest by the government; told that your money is being stolen and you will lose access to your bank account; or notified that utility services or accounts will be cancelled. There is generally an "emergency" where you directed to act or send money right away or you will lose the promised benefit, or suffer a negative consequence (law enforcement will arrest you, your money will be lost forever, a loved one will be injured, etc.). The pressure to act immediately, a request to keep things secret, and suggestions on what lies to tell to the bank and others are all significant red flags of fraud. The latest schemers grab your attention by claiming that you or your money have been linked to cartel crimes or crimes involving children.
- The scams and the tone of the fraudsters are increasingly more threatening. When scammers get you on the phone, they will make threats to keep you on the phone and may falsely claim your telephone and computer are "tapped," so you do not have time to think about what you are doing and cannot learn they are scammers. Everyone is receiving calls from fraudsters, so practice your response: learn to "accidentally" hang up, or tell them, "I am so sorry — I have just had a personal emergency and will call you right back!!" Always research to find legitimate telephone or website contact information to follow up on any notices or calls, and be aware that the first responses to internet searches are generally advertisements that can contain fraudulent links. Legitimate callers will never be offended if you call them back later.
- Be aware that fraudsters routinely impersonate law enforcement officials such as police officers, detectives, FBI agents, and other government investigators. No law enforcement officer will ask you to participate in any investigation by providing them with your personal/

financial information, sending money to anyone, or giving them valuables to hold, such as gold. Under no circumstance should you meet with anyone to give them cash or gold — it is a scam!

- Do not be tricked into becoming a "money mule" to help fraudsters steal money. All legitimate businesses and people have access to some sort of banking or financial system. Only a fraudster will ask you to use your bank account to receive money and send it out to others.
- No legitimate bank or government official will ever ask you to take money out of your account as cash, ask you to purchase a money order/cashier's check, or ask you to purchase gold to "protect your assets." Immediately contact your local law enforcement agency if this occurs.
- Fraudsters can take control of your bank accounts and take all of your money if you allow them to connect to your computer, tablet, or phone. No bank will ever ask you for your login ID, password, or the multi-factor authentication code the bank sends you by email or text. Only fraudsters trying to steal your money will ask for these things. They may have access to your login and password due to a database breach, but they cannot move money unless you give them the code — don't do it!
- Computer pop-up messages that direct you to email someone, click on a link, or call a phone number to handle a computer security or other threat are *always scams*. Do not email, click the link, or call the phone number. Simply close your internet browser. *Never* allow anyone online access to your computer or account (by clicking on a link or providing login name and passwords). Only scammers ask for direct access to your computer.
- No legitimate company or agency will ever direct you to pay with a gift card you purchase from a store, send a bank transfer to a person using Zelle/Cash App/Venmo or similar service, or send cryptocurrency (Bitcoin). Only fraudsters will ask someone to mail cash. Any request to deposit cash *into* an ATM (Crypto Kiosk) for payment, investment, or to secure money is a *scam to steal your money*. Once sent, the money generally can never be recovered. You should never have to pay taxes or fees to receive money such as a loan or an inheritance; funds are always deducted and paid ahead of time, paid directly from the estate, or become your obligation only after you receive all of the money.
- Regularly back up all digital records to an external storage device and/or digital cloud storage. Ransomware, computer viruses, power surges, and aging drives can destroy files at any time.
- Use "strong" passwords to protect your information. Strong passwords are a combination of letters, numbers, and symbols and contain at least 12 characters (longer passwords are more secure). Never use personal or family names or dates. For highest security, do not save login usernames and passwords on your browser — type them in each time you use the computer. Consider using password management software to track and store passwords and fill in login forms securely.
- Credit card companies, banks and other financial institutions, and government agencies (IRS, Social Security, etc.) will never contact you and ask for personal information (other than passphrases). Your Social Security number can never be cancelled, and you are not responsible for anyone falsely using it. It is illegal to enter a foreign sweepstakes or lottery.
- Keep your security software updated. Personal firewalls and security software packages (with anti-virus, anti-spam, and spyware detection features) are a must-have for everyone

who uses a computer or cellular phone. Also, make sure your computer has the latest updates and security patches for the operating system.

- ✦ Make sure that you access your online accounts only on a secure webpage using encryption. The website address of a secure website connection starts with "https" instead of just "http" and has a key or closed padlock in the status bar. Public WiFi is not secure unless you also use a VPN (Virtual Private Network) connection.
- ✦ Never post identifying information about you or your family on your personal website or social media sites. Ensure your privacy settings secure your accounts.
- ✦ Be aware that we are losing more and more money each year to consumer fraud schemes where scammers trick us into sending money for fake products, false vacation rentals, and other online purchases. You never really know who is on the other end of the keyboard, so do your homework and be careful before making a purchase. A deal can be too good to be true.
- ✦ Always use a credit card when making online purchases rather than a debit card. Never pay with cash, a check, money order, wire transfer, or cryptocurrency because you will never get your money back if it is a fraudulent transaction. Report fraudulent use of a credit card or debit card immediately to limit or eliminate your liability.
- ✦ Your cellular phone is a computer. Anyone you allow to use your phone can quickly access all your personal and financial information, transfer the information to others, change email and account passwords, and use banking applications to take money from your accounts. Never give your cellular phone to a stranger for any reason.
- ✦ Never authorize a transfer or wire money without being certain the destination account number really matches the destination person or company. Contact the destination bank directly using a trusted phone number and confirm the actual name on the account. Fraudsters are using emails, texts, and phone calls to impersonate company owners/managers, customers, clients, escrow agents, and bank employees to trick victims into wiring money to a scammer's bank account, and the funds can rarely be recovered.
- ✦ If you are the victim of a crime, please make a report to your local law enforcement agency immediately. Contact the Colorado Bureau of Investigation to report check and wire fraud with 48 hours. Crimes involving the internet and computers can also be reported to the Federal Bureau of Investigation at www.ic3.gov.

23-4. Protection from Abuse

You do not have to accept threats or abuse from anyone, including your family. If someone close to you has threatened you with violence or abused you in any way, there are state laws in place to protect you. A **protection order** can be issued through the district court, county court, probate court, juvenile court, or a qualifying municipal court in the city or county where you live, the abuser lives, where one of the parties is employed, or the abusive acts occurred that restricts that person from having contact with you or continuing the abuse under certain conditions. There are both civil and criminal protection orders and each applies under the following circumstances.

Criminal Protection Orders: C.R.S. § 18-1-1001. When an abuser has been charged with a crime under Title 18, a mandatory protection order is automatically put into place to protect the victim from the abuser and will stay in place for the duration of the court proceeding through the end of the abuser's sentence. If you are a victim or witness to a crime, you may contact the prosecutor to request a full no-contact order, an order for the offender to vacate the home, or other additional conditions to help you. A court may order GPS monitoring, monitored drug or alcohol sobriety, and other conditions to keep a victim safe.

Civil Protection Orders: C.R.S. §§ 13-14-100.2, *et seq.* If you are being physically or verbally threatened by an abuser, you can ask the court to protect you by requesting that a civil protection order be issued against that abuser. Civil protection orders are especially appropriate when the abuser has not been charged with a crime. Court forms and instructions are available at https://www.coloradojudicial.gov.

For various reasons, actions taken by an abuser may not be reported to law enforcement or charged in a criminal case. Under these circumstances, if you fear for your safety or the safety of others, civil protection orders can offer you safeguards. Under Colorado law, a court may issue a temporary or permanent civil protection order against an adult or juvenile over the age of 10 for any of the following purposes:

1) To prevent assaults and threatened bodily harm;
2) To prevent domestic violence and abuse;
3) To prevent emotional abuse of the elderly or of an at-risk adult;
4) To prevent sexual violence; and
5) To prevent stalking.

The protection order can issue against almost anyone: a stranger; a current or former relative by blood or marriage; someone who lives or has lived with you; a caregiver; or a spouse or someone you are, or have been, intimately involved with.

The judicial officer (judge or magistrate) can issue emergency oral protective orders, a temporary protection order, or a permanent protection order that directs the restrained person to stop doing something, to refrain from doing something in the future, or even to take certain actions to benefit the protected person. A temporary protection order may issue if the judicial officer finds a risk or threat of physical harm or the threat of psychological or emotional harm exists to the person(s) seeking protection.

To obtain a protection order, you may need to appear in person before the judicial officer and testify, submit a notarized/verified affidavit of facts from you and/or additional witnesses, produce copies of business or official records, or have other witnesses testify. Through the civil protection order process, you can request that the judge or magistrate issue specific orders to address the abuse and harm you are suffering, including orders to the restrained person to stop:

- Verbal threats or assault;
- Physical or verbal harassment;
- The inappropriate use or the threat of inappropriate use of medications;
- The inappropriate use of physical or chemical restraints, including locked doors; or
- The misuse of authority granted by a power of attorney, a guardianship, or a conservatorship that results in unreasonable confinement or restriction of an elder 60 years of age or older.

The protection order can require the restrained person to:

- ✦ Vacate the family home and stay away from any location the protected party is known to be; or
- ✦ Preserve or maintain the health and well-being of the protected person's animal or pet by not threatening to commit or committing any act of violence against the protected person's animal or pet, or otherwise taking, transferring, concealing, harming, or disposing of the animal in order to coerce, control, punish, intimidate, or exact revenge upon the elder, at-risk adult, or current or former domestic partner.

The necessary forms and instructions for protection orders are available at the courthouse or available online and should be filed in the county or municipality where the abuser lives, where any one of the acts or behaviors you are seeking to stop occurred, where you live, where you work, or where the abuser works. The filing fee and sheriff's fee for personal service on the defendant/respondent can be waived if you cannot afford to pay them. You can contact victim assistance agencies to accompany you and assist you with the paperwork. Your local police department, district attorney's victim assistance staff, and county department of human services can provide contact information for individuals who can assist you. They also can refer you to safe shelters and other services.

See also Chapter 28, "Mandatory Reporting of Elder Abuse or Exploitation."

23-5. Resources

Colorado Crime Victims Compensation Programs: *See* section 22-6, "Resources"