Business Protection Tips

BUSINESS ROBBERY AND BURGLARY PREVENTION

Robbery is the felonious taking of personal property in the possession of another, from his person or immediate presence, and against his will, accomplished by means of force or fear. Robbery is a violent crime and often includes the use of a weapon. Robbers often case businesses for cash on hand and ways to achieve surprise and avoid witnesses. Burglary is the entry of a business or other property with the intent to commit larceny or any felony. Businesses can prevent robberies and burglaries by protecting assets, preventing unauthorized entry, and employing various deterrent measures. They can also help in apprehending the offenders and recovering the stolen property. This page also includes tips on what to do if you are robbed.

These tips can significantly enhance the safety of your employees and the security of your business. The NPD Crime Prevention Coordinator will be glad to assist you in this by doing a free business security survey.

Apprehending Robbers

- Observe carefully all suspicious persons or vehicles so you can provide a good description of them if they commit a crime. Be aware that criminals might be using physical disguises, e.g., wigs, mustaches, etc.
- Place colored height marks at all exit doors to help employees estimate the height of suspicious persons.
- Develop a mutual aid system. Form an agreement with nearby merchants to keep an eye on each other's businesses and watch for suspicious activities. An inexpensive buzzer system can alert adjoining businesses to an emergency situation.
- Install cameras that can provide good imagery of persons entering and leaving the business and committing a crime in the business. The imagery quality should enable the criminal to be identified.
- Monitor cameras to enable crimes in progress to be observed and reported, and actions taken to stop and apprehend the criminals before they can escape.
- Install silent panic alarm buttons at cashier and other vulnerable positions.
- Install two sets of doors and a remote locking system to enable an escaping criminal to be trapped between them.
- Make address numbers easy to read from the street to avoid delays in police response. They must be on a contrasting background and located above the doorway or in a position where they are plainly visible and legible from either direction of approach from the street fronting the property. They should be at least 12 inches high on commercial buildings and lighted at night. Additional numbers are recommended on the rear doors so they can be seen from alleys.

- Where address numbers are not easily visible from the street, e.g., for businesses in a shopping mall, additional numbers should be posted where they will be visible.

Deterring Crimes

Crimes can be deterred by having good visibility in the business and on the premises, alarm systems, surveillance cameras, security guards, dogs, and good lighting, and keeping the property in good condition, posting signs, etc.

Visibility

Good visibility in and around the business creates a risk of detection for intruders and offenders, and a perception of safety for persons legitimately on the premises.

- Provide two-way visibility in areas open to the public. Keep windows and counters clear. Don't allow them to be cluttered with signs, displays, plants, etc.
- Provide one-way visibility from the inside in areas not open to the public. Use mirrored glass or see-through curtains to maintain inside privacy. Use glare-proof glass to enable occupants of a lighted building to see out at night.
- Install convex mirrors to enable employees to see people in areas that might be blocked by display shelves, walls, or other obstructions.

Alarms

Install a good alarm system. One will usually include one or more of the following components: magnetic contacts on doors and windows, photocell or pressure sensors with annunciators at unlocked or open doors, heat or motion detectors in interior spaces, glass break detectors, keypads with a means of checking the status of the system, and audible alarms. All equipment should be Underwriters Laboratory (UL) certified.

- Multiple sensors are preferred because they reduce false alarms, which are wasteful of police resources and can lead to fines.
- Get alarm company references from other businesses. Get at least three estimates in writing. The NPD does not prefer or recommend companies, brands, or types of security systems.
- If your system is monitored, make sure the monitoring station is open 24/7 and has backup power. The company's customer service department should also be open 24/7.
- Make sure you understand your service contract, all the points of protection and the equipment to be installed, the initial and monthly payments, and the warranty period.
- Inform your insurance company. You may qualify for a discount.
- Harden the telephone line that sends the alarm signal to the alarm company so it cannot be cut from the outside. And if it is cut, have the system send an alarm to the alarm company. If the telephone line is contained in an outside box, the box should be alarmed or locked with a shielded padlock. Or the system could have a wireless backup that would send the alarm if the telephone wire were cut.
- The system should also have a fail-safe battery backup. Check the batteries periodically and replace them if necessary.

Surveillance Cameras

Criminals may be deterred from committing a crime if they know that their actions are recorded on a camera. Or they may be prevented from committing a crime if preventative measures can be taken soon after they are observed entering your property or business.

- Install cameras to record people entering and leaving the business and committing a crime in the business. Cameras should be mounted where they cannot be covered or tampered with. Dummy cameras should not be used because most criminals can tell the difference between real cameras and dummies.
- Observe what is happening outside your place of the business. Look for anyone watching or loitering near it.
- Install cameras to record people and vehicles in your parking lot.
- Install video analytics or intelligent video software in your camera system. It will alert you when something suspicious appears on your monitors, so you don't have to watch them all the time. The monitors could be located at your business or at a security company office. In the latter case an Internet link to transmit the imagery would have to be provided. The NPD could then be called if a crime is observed. Officers might even arrive in time to catch the perpetrators.
- Lights could be turned on when motion is detected in outside areas that are secured at night, and audio announcements made to warn trespassers that the police would be called if they do not leave the property immediately.
- If signs stating that security or surveillance cameras are installed are posted and the cameras are not monitored all the time, the sign should also include that caveat. This is important in keeping people from having a false sense of security and expecting help in the event they are attacked.

Any camera system that is installed should be designed to provide high-quality, digital imagery of suspicious persons and activities for use by the NPD in investigating crimes.

Security Guards

Consider employing well-trained, highly visible security guards. Uniformed security guards that patrol the business on foot can be a highly effective in deterring robberies and burglaries. Make sure that the guards are from a licensed and insured company. The guards should be licensed as well.

Dogs

Dogs act mainly as a psychological deterrent. They can be an excellent supplement to a security system provided the animal can be relied upon to give warning when warning is needed. Dogs can scare a stranger away by either barking or looking fierce. But remember that they can be lured away, poisoned, killed, or even stolen. Trained attack dogs are not recommended because the risk of liability to the owner is great should the dog attack an innocent person. Outside dogs should be kept in a fenced area with a good lock on the gate.

Lighting

Illuminate all external areas of your property at night, especially parking lots and storage yards. And leave a few interior lights on in the back of the store or office where they may illuminate and silhouette intruders but not create glare for passing patrol cars.

- Timers or photoelectric cells can be used to turn lights on at dusk and off at dawn. And motion sensors can be used to turn lights on when any motion is detected. Streetlights or lights from adjoining properties should not be relied on for lighting the property at night. Also, the lights should be directed so they don't shine into the eyes of passing motorists or police patrols.
- Replace burnt-out bulbs promptly. Use screens, wired glass covers, or other protection for light fixtures and bulbs. Install padlocks on circuit-breaker boxes to prevent the lights from being turned off.
- Because lights and other security systems work on electrical power it is important that measures be taken to prevent disruption of external power or provide internal backup power. At a minimum, external circuit breakers should be installed in a sturdy box that is locked with a shielded padlock.
- Trim trees and bushes so they do not block lighting.

Property Condition

Keep your property in good condition. Criminals are attracted to property in poor condition because it shows that the owners or tenants don't care about it.

- Keep property free of trash, litter, weeds, leaves, dismantled or inoperative vehicles, and other things that indicate neglect.
- Replace or repair broken windows, screens, fences, and gate locks.
- Remove loose rocks and other objects that could be used to vandalize your property.
- Keep outside trash dumpster enclosures and the dumpsters in them locked when not being filled or emptied.
- Remove graffiti as soon as possible after it is found. This will discourage further vandalism. The graffiti should be covered with matching paint, so a "canvas" is not left for the vandals. Hardware or paint stores should be consulted regarding the best products for removing various types of graffiti from specific surfaces without damaging the surface. Extreme care should be used in applying special graffiti removal products like MEK (Methyl Ethyl Ketone) or “Graffiti Remover” on glass or unpainted surfaces.
- Install a protective film on the outside of windows to prevent window damage from graffiti, knife gouging of scratching, and acid etching.
- Keep landscaping trimmed to preserve good visibility on the property and deny criminals possible hiding places. Trim bushes to less than 3 feet, especially near windows, sidewalks, and exterior doors. Trim tree canopies to at least 8 feet.
- Use fencing, gates, landscaping, pavement treatment, signs, etc. to define clear boundaries between your property and adjoining properties.

Preventing Unauthorized Entry

The following tips suggest how to prevent unauthorized entry to your business. They deal with doors, locks, windows, security gates and shutters, other openings, roofs, fences, walls, gates, and landscaping. Make sure that all protective measures installed meet the fire and life safety standards for your type of building. You can contact Neenah-Menasha Fire Rescue 886-6221 for assistance. This will assure safety and code compliance as well as enhance your security.

Doors

Exterior doors can be wood, metal or glass. Solid doors should be at least 1-3/4 inches thick.

- Reinforce wooden doors with 16-gauge sheet metal for added security.
- Use reinforced or strong glass, i.e., laminated glass or clear acrylic plastic, in exterior glass doors. The former has plastic sheets between layers of glass. It looks like safety glass but will not shatter easily, even after repeated blows. The latter is also shatterproof but has several disadvantages. It comes in limited sizes and is susceptible to marring and scratching.
- Install a 180-degree peephole in solid doors so you can identify persons at the door without them seeing you. It also enables you to check that no one is hiding near the door before it's opened, e.g., to take out trash.
- Hinges should be located on the inside or have non-removable pins.
- Where motion detectors are installed to open or unlock exit doors from the inside when a person approaches the door, make sure the detectors are set far enough back from the door so a person outside the door cannot slip something between the door and the frame to create motion on the inside and thereby open the door. Or install a shield on the outside of the door so a person on the outside cannot slip anything between the door and the frame.

Locks

Doorknob locks offer no security. Defeating these locks is one of the most common means of forced entry. All exterior doors should have a single-cylinder deadbolt lock. Go to a locksmith or hardware store for advice on locks.

- Bolts on deadbolt locks should have a minimum throw of 1 inch. Strike plates should have screws that are at least 3 inches long.
- Install flush bolts at the top and bottom of all double doors. These should be made of steel and have a minimum throw of 1 inch.
- Secure sliding-glass doors to prevent both horizontal and vertical movement. Deadbolt locks provide the greatest security. Less effective secondary locking devices include a pin in the upper track that extends downward through the inner doorframe and into the outer door frame, a thumbscrew-type lock mounted on the top or bottom track, and a metal strip or a few metal screws in the track above the door to prevent vertical movement.
- Install deadbolt locks all doors that lead outside through garages or storage areas.
- Re-key or change all locks when moving into a new location.
- Install good locks on gates, garages, sheds, etc. If padlocks are used, they should be keyed and able to survive assaults by bolt cutters or pry bars. The shackles should

be of hardened steel and at least 9/32 inch thick. It is even better to use a "shielded" padlock that is designed to protect against bolt cutters. Combination locks should not be used because they offer very poor security.

- All locks should be resistant to "bumping."
- Use a multi-frequency opener on electrically operated garage doors, and make sure that the bottom of the door cannot be lifted up to allow a burglar to crawl in.
- Use hardened steel hinges, hasps, and padlocks on hand-lifted garage doors.
- Install cane bolts or sliding hasps on the inside of garage doors to provide additional security.
- Consider installing a crossbar as an additional locking mechanism for exterior doors that have in interior swing. Place a metal bar or 2- x 4-inch piece of wood in brackets mounted on both side of a door. Slide bolts of heavy gauge steel can also be effective.
- Use panic deadbolts operated by push-bars to secure secondary exits that are designated for emergency use only. They can be alarmed to ring a bell or sound a horn when the door is opened.
- Install latch guards. They are steel plates that are bolted to the frame of the door to prevent the locking mechanism from being defeated. They also prevent objects from being inserted between the door and the frame that could damage the door itself. More expensive guards protect the mortise cylinder and prevent a burglar from drilling out the tumblers.

Windows

Do not rely on the locking means supplied with your windows. Additional security measures are usually necessary.

- Secure double-hung sash windows by drilling a hole that slants downward through a top corner of the bottom window into the bottom corner of the top window on both sides of the window. Place an eyebolt or nail in the hole to prevent the window from being opened.
- Replace louvre windows with solid glass or some other type of ventilating window. If this cannot be done, glue the panes together with a two-part epoxy resin.
- Secure casement windows with key-locking latches. Make sure that the protrusion on the window that the lock is attached to is made of steel and not worn, and that the window closes properly and is not bowed or warped.
- Secure sliding-glass windows by the same types of locking devices used for sliding-glass doors.
- Consider installing security bars on side, rear, or other windows that a burglar might break to enter your business. Make sure that the retaining bolts cannot be removed from the outside. Bars must comply with Fire Code requirements for inside release to permit an occupant to escape in the event of a fire.
- Use reinforced or strong glass. i.e., laminated glass or clear acrylic plastic, in viewing windows on the lock sides of doors so a burglar cannot break them and reach in to open the door.
- Use reinforced or strong glass in display windows to prevent window-smash burglaries.

- Eliminate small windows at ground level that a burglar can break and crawl through, especially where there are low bushes in front of the windows. Or use reinforced or strong glass, or some strong opaque or reflective material in them.
- Install bollards in front of windows and doors to prevent vehicles from driving in.

Security Gates and Shutters

Folding security gates and roll-down shutters inside windows and doors provide additional security. A burglar would have to cut through the bars or slats after breaking through a window or door to enter the business all while the alarm is going off. The presence of gates or shutters would be a strong deterrent of break-ins.

Other Openings

All crawl spaces, ventilation windows, and other openings should be secured to prevent access through them.

- Make sure that window air conditioners are installed securely and cannot easily be removed from the outside. Seal mail slots in doors if a coat hanger or other device can be inserted and used to release the door lock.
- Secure or alarm hollow walls or attics that are shared with an adjoining business.

Roofs

Ladders, trees, fences, drainpipes, and adjoining rooftops can provide roof access if measures are not taken to deny such access.

- Shroud ladders with locking covers.
- Trim tree limbs that could provide access.
- Secure rooftop skylights, ventilation shafts, air conditioning and heating ducts, and other possible entry points on the inside with grills or grates. Those that cannot be secured should be alarmed.

Fences, Walls, and Gates

Well-built fences, walls, and gates are the first line of defense against criminals. Follow all code requirements when constructing.

- Install open chain link or ornamental metal fencing unless privacy and noise reduction are needed. These types are preferred because they do not block visibility into the property and are less susceptible to graffiti. Chain link fencing should have its bottom secured with tension wire or galvanized pipe, or embedded in concrete to prevent it from being lifted up to enable a person to crawl in. The horizontal bars on ornamental metal fences should be located only at the top and bottom on the inside of the fence. Fences should be at least 6 feet high.
- Sharp-pointed fencing is only permitted in agricultural zones but in special situations it may be allowed to exist in industrial zones.
- Equip gates with good locks. Latches should be mounted with carriage bolts and nuts that are welded on or secured by stripped bolt threads.

- Gates that are opened on the inside by a handle or knob should have shields that prevent a person from reaching in to open them. They should also be tall enough so that a person cannot reach over the top to open them.
- Gates with beveled latches should be shielded so a person cannot insert a wire or bar between the frame and the gate and push in the latch. The shield should be centered on the latch. A dead-bolt lock with a cylindrical latch would be even better on gates that are not emergency exits and are closed and locked manually from the outside.
- Gates that are opened on the inside by a push bar should be solid or have a solid metal or plastic shield on the inside of the gate that extends at least two feet above and below the push bar. The shield will prevent a person from opening the gate from the outside by looping a wire through the gate and pulling on the push bar.
- Exit gates should have springs that close them securely after a person goes through. Sensors should also be installed to warn the security office or manager that a gate has been left open.

Landscaping

Defensive plants can help in access control.

- Plant bushes with thorns or prickly leaves under ground-level windows to make access more difficult for burglars.
- Plant bushes with thorns or prickly leaves along fences and walls to make climbing more difficult and prevent graffiti.

Protecting Assets

Assets can be protected by keeping them in a safe place, implementing procedures that deny criminals access to them, etc.

- Locate the cash register where it is visible from the outside, but far enough away from the window so as not to provoke a quick window-smash and grab.
- Protect cashier with a bullet-resistant glass, plastic, or laminate enclosure or window. And install a secure money pass-through slot or tray.
- Keep a minimum amount of cash in the register. Close registers after each transaction. Lock registers when not attended.
- Put excess cash in a time-lock drop safe. Keep your safe locked when access is not required.
- Safes can be standing or mounted in floors or walls. Standing safes should be securely anchored to the floor. The back should be against a wall so it will not be accessible. Safes that are visible from outside the building should be well illuminated and have the front (locking side) turned away from the windows. Floor safes should be located where they can be concealed.
- Use burglar-resistant safes for money and other valuables. Use fire-resistant safes for records. Both types should have an Underwriters Laboratory (UL) label with their effectiveness ratings.
- Post signs saying that employees do not have access to the safe.
- Lock up postage meters, check writers, checkbooks, etc. when they are left unattended.

- Be unpredictable about moving money from your business to the bank. Vary the times, routes, and methods of concealment. Make deposits during the business day, not after closing time. Assign two employees to make deposits. Vary the assignments over time. Have the deposit carried in a purse or plain bag; never use a bank bag.
- Have employees leave the depository if suspicious persons are present. Have them return and make the deposit later.
- If you use an armored car service, always be prepared for their pickup and delivery.
- Designate one or better two employees to open and close the business.
- Have two employees open and close the business if possible.
- Have at least two employees working at high-risk times.
- Be especially alert at opening and closing times when the business is not crowded.
- Be careful in dealing with customers who are wearing baseball caps and sunglasses that conceal their faces from surveillance cameras.
- Never open your business for anyone after you have closed. Beware of the caller who states your business has just been broken into and asks you to come down. Always call back to confirm that the call was from a law enforcement agency or your alarm company before going to your business.
- Keep all exterior doors locked during business hours except those used by the public. Some employees or security guards should be located to monitor each public entrance. Emergency exits should be alarmed and designated for emergency use only. Have employees report and close any exterior door found open in areas not accessible to the public.
- Lock stairwell doors to areas not accessible to the public. Install card readers for employee access to these areas.
- Post signs to indicate areas that are open to the public and those that are for employees only. Install locks on all doors to interior work areas to control public access. Doors to storage and supply rooms, and individual offices should be kept locked when unattended.
- Check all restrooms and other areas at closing time to make sure no one is hiding in them.
- Have all employees wear ID badges or some other means of distinguishing them from visitors, customers, and others on the premises. Businesses with restricted areas should give their employees photo-ID badges that are color-coded to indicate the areas that the employee is authorized to enter. Offices, storage and supply rooms, and other work areas should be checked periodically for the presence of unauthorized persons.
- Keep doors to public restrooms locked or under observation to prevent abuse of the facilities.
- Anchor computer hardware and other costly items of office equipment to a desk or install an alarm that sounds when they are moved. Otherwise store the equipment in a secure place when it is not in use.
- Keep items stored outside at least 8 feet from perimeter walls and fences. Forklifts, moving equipment, and other vehicles that can easily be started should be made inoperable.

- Park company vehicles in a secure fenced area when the business is closed. If this is not possible, park them close to each other or against the building to help prevent gas siphoning, battery theft, and vehicle break-ins. They can also be parked in front of doors to prevent building break-ins.
- Keep shipments inside until they are to be loaded on trucks.
- Open loading dock doors only when shipments are being sent out or brought in. Keep the doors locked at other times.
- Install a service bell for truck drivers to use to announce their arrival.

Recovering Stolen Property

- Place the company's name or some identification number on all company-owned items, e.g., office equipment, tools, vehicles, and machinery. This can be done by engraving or etching, using a permanent adhesive, or by attaching microdots. In small individually owned businesses, the owner's drivers license number can be used as a property identifier.
- Use "bait money." Keep a list of serial and series numbers. Do not use these bills to make change.
- Place numbered confetti in bulk goods containers.
- Contractors can get information on preventing thefts of construction equipment and recovering stolen equipment by calling the Construction Industry Crime Prevention Program at **(562) 860-9006** or visiting its website at www.crimepreventionprogram.com.
- Keep a detailed, up-to-date record of your valuables. Include type, model, serial number, fair market value, etc. Photograph or videotape all valuables.

Visitor Control

Visitor control is relatively simple in some businesses, e.g., medical offices. Patients, salespeople, etc. are free to enter the building, go to their doctor's office, and check in with the receptionist. Then they are allowed to proceed to the examination rooms. Signs would be posted to indicate areas that are not open to visitors, i.e., storage and supply rooms, and individual offices, which should be locked when unattended.

Other businesses have visitor control in the building lobby where a receptionist or security guard processes visitors, who can be clients, patients, meeting attendees, salespeople, business guests, contractors, delivery and service persons, or employee family members. In this case visitor processing would include the following four tasks: identification, validation, screening, and monitoring.

- Establish and verify the visitor's identity. A government-issued, picture ID, e.g., a driver's license, is usually acceptable. If a visitor does not have an ID, his or her host might be asked to come to the lobby and vouch for the visitor's identity.
- Validate the visitor's purpose. This is usually done by calling the visitor's host.
- Check the visitor's personal and hand-carried items. Screening is usually done by looking into bags and briefcases. More extensive screening may be appropriate in

some buildings. This would include metal detectors, package x-ray machines, and explosive detectors.

- Once a visitor has been identified, validated, and screened, his or her movement within the building may need to be monitored. Procedures range from none, i.e., the visitor has complete freedom to go anywhere in the building, to being escorted everywhere. In most cases a visitor will be issued and required to wear a badge. In addition to the visitor's name and date, the badge could also have the host's name, the area(s) of the building to which access is allowed, and the visitor's picture. If an escort is not provided, a badge is only useful of all building employees are also required to wear a badge. Otherwise, a visitor can remove the badge and look just like an employee.
- Where visitors and employees are required to wear badges, train employees to challenge and offer assistance to any person not wearing a badge.

What To Do If You Are Robbed

Every robbery is different. You will need to assess yourself, the robber, and the situation to determine what you should do. Here are some general tips to use in training your employees:

- Act calmly. Do exactly what the robber says. Keep your movements short and smooth to avoid startling the robber.
- Do not resist. Cooperate for you own safety and the safety of others. Robbers usually are excited and easily provoked. Tell the robber about any movements you plan to make.
- Activate an alarm if it can be done safely without alerting the robber.
- Observe carefully. Study the robber's face and clothing, note any other distinguishing features, observe the direction of escape, record the license, make, and color of any vehicle used in the robbery, etc. Write down everything you can remember about the robber and the crime itself.
- Lock the door and call **911** immediately after the robber leaves. Then you can make other calls.
- Preserve the scene. Discontinue regular business until officers have searched the scene. Cover any surfaces the robber may have touched and keep away from areas where the robber may have been.
- Ask other witnesses to remain. Get names and phone numbers if they are unable to remain. Ask to see their driver's licenses or other ID to verify this information.
- Save camera imagery records.
- Don't discuss the robbery with others until all statements have been taken.

Preventing Internal Theft in Businesses

Employee theft is very common. Some retail industry studies have found that more than one-third of all thefts from businesses were by employees. One way of controlling theft is to develop a good relationship with your employees. Make them feel respected and reward them for doing their jobs well. Provide good career opportunities. Companies with the lowest turnover rates have been found to have the lowest internal theft rates. Other ways to prevent internal theft are outlined on this page.

Despite your best efforts, dishonest employees can usually find ways to steal. If you suspect theft, call your security or loss prevention personnel and then the Neenah Police Department. Don't play detective and try to solve the crime. And don’t jump to unwarranted conclusions. A false accusation could result in serious civil liability.

Access Control Cards

- Replace keys with access cards where practical. Cards are preferred because a record can be kept of their use, they cannot be duplicated and given to unauthorized persons, they can be deactivated when reported missing or when the employee's authorization ends, their use can be limited to specific doors by time of day and day of week, and they can also be used to open parking lot or structure gates.
- Deactivate missing, lost, or stolen cards immediately on notice.
- At least annually, check that employees have their cards.
- Do not allow contractors and cleaners to keep cards. Have them sign out for and return them on a daily basis where practical.

Bank Deposits

Use an armored car service if possible. Otherwise assign two employees to make deposits. And vary the assignments over time.

Cash Handling

- Provide a receipt for every transaction. Encourage customers to expect a receipt by posting signs at each register.
- Put one employee in charge of setting up cash drawers. Have another double-check the cash count.
- Make each employee responsible for his/her cash drawer. Issue one cash drawer to each on-duty employee. No other employee should be allowed to open or use another's cash drawer at any time. At the end of each shift each cash drawer should be balanced by the employee and double-checked by another.
- Require that the cash register drawer be closed after each transaction. Never leave a register unlocked when not attended. And never leave the key with a register.
- Identify each over-ring and under-ring. Managers should sign off all voids and over-rings.
- Check signatures against those on file.
- Limit the amount of cash accumulated in any register. Use a drop-safe for excess cash.
- Check cash-to-sale ratios. These, along with unusually frequent refund transactions, can indicate employee theft.
- Keep tendered bills on the register until the transaction is concluded. Short-change artists frequently pay with large bills.
- Conduct only one transaction at a time. Do not be intimidated into rushing.
- Check for counterfeit currency. The look of the paper and its "feel" are usually the most obvious signs. A common counterfeiting practice is to "cut corners" off large bills and affix them to small-denomination bills. Inexpensive devices are available to aid detection of counterfeit bills.

Document Protection

- Shred all potentially sensitive materials including customer lists, price lists, medical prescription receipts, invoices, computer outputs, and documents with signatures.
- Require that all desks be cleared of important or confidential documents at night and when their offices are unattended.
- Require that all file cabinets be locked when not in use.

Employees Property

- Discourage employees from bringing items that are irreplaceable or have personal value to their offices.
- Warn employees to keep unattended purses, wallets, cell phones, etc. in locked drawers or cabinets.

Inventory Control

- Conduct inventories often and at irregular intervals. Also make routine spot checks.
- Inspect records of purchases and sales at the beginning and end of each shift.
- Define individual employee responsibilities for inventory control. This establishes a climate of accountability.

Key Control

- Appoint a key control officer to manage the key and lock system.
- Keep keys in a locked cabinet or a secured area when they are not in use.
- Minimize the number of master keys issued. Individual offices and restricted work areas should have separate keys.
- Issue as few keys as possible. Issue them only for areas the employee is authorized to be in. Keep up-to-date records of keys issued.
- Caution employees not to leave keys with parking lot attendants, in a topcoat hanging in a restaurant, or in their offices or work areas. This helps prevent keys from being taken and duplicated.
- Stamp a number on each key and have employees sign for keys when they are issued. At least annually check that employees have their keys.
- Also stamp keys DO NOT DUPLICATE.
- Code each key so that it does not need an identifying tag.
- Require departing employees to turn in all issued keys.
- Investigate all key losses.
- Re-key locks whenever a key is lost or when an employee leaves the business.
- Consider installing locks that are inexpensive to re-key. Or better to have a key-card system in which codes can be changed easily when a card is lost, entries and exits are recorded, etc.
- Seek advice from professional access control system designers.
- Do not allow contractors and cleaners to keep keys. Have them sign out for and return them on a daily basis where practical.

Personnel Policies

- Conduct a thorough background check and interview all job applicants. Consider using an outside screening service to collect information on applicants. Test applicants for honesty as well as job skills.
- Adopt a strict code of conduct for employees. Make sure all employees are aware of it. The code should include rules regarding employee purchases of store merchandise.
- Inform employees about internal security measures, e.g., surveillance and inventory checks, and the likelihood and consequences of being caught stealing. Many employees steal because they think they can easily get away with it.
- Keep a record of all employee purchases, exchanges, and refunds. Employees should not be permitted to ring up their own transactions.
- Provide lockers for employees. Require that employee's personal property and any store purchases be kept in their lockers during working hours.
- Prohibit employees from wearing or using store merchandise without purchasing it.
- Limit employee access to the building to the hours that they are scheduled to work.

Purchasing Procedures

- Centralize purchasing but keep it separate it from receiving and accounting.
- Control purchase orders by pre-numbering them in sequence.
- Require supporting documentation for each purchase or expense invoice.
- Use pre-numbered checks in sequence.

Shipping and Receiving Procedures

- Establish receiving procedures that specify where vendors are allowed to park and enter the business.
- Do not permit trucks on the dock until they are ready to load or unload.
- Check all shipments against bills-of-lading. Number shipping orders in sequence to prevent padding or destruction.
- Recheck all incoming goods to prevent collusive thefts between the driver and the employees who handle the receiving.
- Do not permit drivers to load their own trucks or take goods from stock.
- Consider installing video cameras on the loading platforms. Locate the monitors where they can easily be seen by supervisors.
- Keep doors locked when no goods are being loaded or unloaded.
- Install 180-degree peepholes in doors to the dock.

Technology Solutions

Employee theft involving gift cards is growing because the cards are like cash, and it is a lot easier to leave a store with a card than an item of merchandise. Cashiers can fake refunds and then use their registers to fill in a gift card, which they take. Or when shoppers buy a card, they give them a blank card and divert the money into a card for themselves. However, the most common type of employee theft is “sweethearting,” where cashiers fail to ring up or scan goods their friends or relatives bring to their register.

Technology solutions to these problems involve data mining programs and surveillance cameras. Data mining is used to determine whether one cashier is refunding far more items than other cashiers. And cameras can show whether a cashier repeatedly gave refunds to the same friend or relative, or whether a cashier failed to run merchandise over the scanner.

Trash Control

- Keep trash dumpsters inside during business hours.
- Check bins at random times for pilfered goods that might have been placed in them for pick-up after the trash is taken out.
- Use clear plastic trash bags. Inspect bag contents for pilfered goods.
- Keep lids of outside trash dumpsters locked during non-business hours. If practical, keep the lids locked whenever the dumpsters are not being filled or emptied.
- Have employees work in pairs in emptying trash. Or have different employees empty the trash from day to day.

CYBER SECURITY FOR BUSINESSES

Computer crimes involve the illegal use of or the unauthorized entry into a computer system to tamper, interfere, damage, or manipulate the system or information stored in it. Computers can be the subject of the crime, the tool of the crime, or the target of the crime.

As the subject of a crime, a criminal would use your computer or another computer to willfully alter the information stored in your computer, add fraudulent or inaccurate information, delete information, etc. Motives for this include revenge, protest, competitive advantage, and ransom.

As the tool of a crime, a criminal would use a computer to gain access to or alter information stored on another computer. In one common mode of attack a hacker would send a "spear phishing" e-mail to employees who have access to the business bank account. The e-mail would contain an infected file or a link to a malicious website. If an employee opens the attachment or goes to the website, malware that gives the hacker access bank account logins and passwords would be installed on the computer. The hacker would then have electronic payments made to accounts from which the money would be withdrawn. Criminals also use computers to commit various frauds and steal identities and other information.

As the target of a crime, computers and information stored in them can be stolen, sabotaged, or destroyed. Sabotage includes viruses, malware, and denial-of-service attacks. Trade secrets and sensitive business information stored in computers can be lost in these kinds of attacks.

Your computers and the information in them should be protected as any valuable business asset. The following tips deal with physical and operational protective measures, Wi-Fi hacking and hotspot dangers, personnel policies and employee training, anti-virus and spyware protection, protecting your bank accounts, use of social media, preventing and dealing with data breaches, and safer use of the Internet. For more details see National

Institute of Standards and Technology (NIST) Interagency Report NISTIR 7621 entitled *Small Business Information Security: The Fundamentals*, dated October 2009. It's available online under NIST IR Publications on http://csrc.nist.gov.

Also, consider joining the FBI's InfraGard, a partnership with the private sector with the goal of promoting an ongoing dialogue and timely communications between its members and the FBI. Its members gain access to information that enables them to protect their assets from cyber crimes and other threats by sharing information and intelligence. Go to www.infragard.net to apply for membership.

Physical Protective Measures

- Do not allow unauthorized persons to have access to any of your computers. This includes cleaning crews and computer repair persons.
- Install surface locks, cable locking devices, and fiber-optic loops prevent equipment theft.
- Install computers on shelves that can be rolled into lockable furniture when employees leave their work areas.
- Locate the computer room and data storage library away from outside windows and walls to prevent damage from external events.
- Install strong doors and locks to the computer room to prevent equipment theft and tampering.
- Reinforce interior walls to prevent break-ins. Extend interior walls to the true ceiling.
- Restrict access to computer facilities to authorized personnel. Require personnel to wear distinct, color-coded security badges in the computer center. Allow access through a single entrance. Other doors should be alarmed and used only as emergency exits.

Personnel Policies and Employee Training

Employees can do a great deal of damage to a business by ignorance of security policies, negligence in protecting business secrets, deliberate acts of sabotage, and the public release of sensitive information. The following measures will help prevent this.

- Conduct a comprehensive background check on prospective employees. Check references, credit reports, criminal records, and schools attended.
- Interview prospective employees. Seek to hire individual who are team-oriented, can respond well to criticism, and can deal well with conflicts, i.e., ones unlikely to become insider threats.
- Require vendors, suppliers, and other contractors to use similar standards in hiring their employees. Include language in all contracts that makes contractors liable for actions of their employees.
- Treat all employees fairly and make sure none are teased by their peers or supervisors because of their ethnicity, speech, financial situation, social skills, or other traits.
- Monitor activities of employees who handle sensitive or confidential data. Watch for employees who work abnormally long hours, weekends, or holidays, or who refuse to

take time off. Many computer crime schemes require regular, periodic manipulation to avoid detection. Also watch for employees who collect material not necessary to their jobs, such as data printouts, software manuals, etc.

- Train your employees in your basic computer usage and security policies. Also cover penalties for not following your policies, and have employees sign a statement that they understand and will follow your policies.
- Train your employees about security concerns and procedures for handling e-mails, clicking on links to websites, responding to popup windows, and installing infected USB drives. For example, they should not: open e-mail from an unknown sender, open unexpected e-mail attachments, click on any links in e-mail messages even if they look real, respond to popup windows, bring back and install "found" USB drives, etc.
- Train your employees to be aware of what others are doing and to report any suspicious behavior that threatens your security.
- Conduct periodic re-training because people forget things. Use pamphlets, posters, newsletters, videos, etc.

Preventing and Dealing with Data Breaches

The five key principles defined by the Federal Trade Commission in its video entitled *Protecting Personal Information: A Guide for Business* at http://business.ftc.gov/privacy-and-security/data-security will help you protect personal information in your business and prevent data breaches. They are: (1) Take stock, (2) Scale down, (3) Lock it, (4) Pitch it, and (5) Plan ahead. You should do the following for each.

1. Take Stock. Know what personal information you have in your files and in your computers.

- Inventory all file-storage and electronic equipment. Know where your business stores sensitive data.
- Talk to your employees and outside service providers to determine who sends you personal information and how it is sent.
- Consider all the personal information you collect from customers, and how you collect it.
- Review where you keep the information you collect, and who has access to it.

2. Scale Down. Keep only what you need for your business.

- Use Social Security Numbers (SSNs) only for required and lawful purposes. Don't use them for employee or customer identification.
- Keep customer credit or debit card information only if you have a business need for it. Don't keep any information you don't need.
- Change the default settings on your software that reads customer's credit or debit cards.
- Review the credit application forms and fill-in-the-blank web screens you use to collect data from potential customers and eliminate requests for any you don't need.
- Use no more that the last five digits of credit or debit card numbers on electronically printed receipts that you give to your customers. And don't use the card's expiration date.

- Develop a policy for retaining written records that is consistent with your business needs and the law.

3. Lock It. Protect the information that you keep and transmit.

- Keep documents and other materials containing personal information in locked rooms or file cabinets.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Create a security policy for your employees when using laptops in and out of your office. (See prior section on Special Measures for Laptops.)
- Control access to your building.
- Encrypt sensitive information you send over public networks or use a secure file transfer service. Don't send personal information by email.
- Run up-to-date anti-virus and anti-spyware programs on all your computers. Use a firewall to protect your computers and network. (See prior section on Anti-virus and Spyware Protection.)
- Require employees to use strong passwords.
- Set access controls so employees only have access to information they need for their jobs. (See prior section on Procedural and Operational Protective Measures.)

4. Pitch It. Properly dispose of what you no longer need.

- Create and implement secure information disposal practices for employees in your office and for those who travel or work at home.
- Train your staff to separate sensitive and other paper records. Dispose of the former by shredding, burning, or pulverizing them. Use cross-cut shredders. The latter can be put in the trash.
- Make shredders available throughout your office, especially next to the copiers.
- Remove and destroy the hard disk of any computer or copier headed for the junkyard. Or wipe them securely.
- Remove and securely wipe hard drives of rented copiers before returning them. Or clear the memory and change the pass codes.
- Destroy CDs, floppies, USB drives, and other data storage devices, or securely wipe them before disposal.

5. Plan Ahead. Create a plan for dealing with security breaches.

In addition to having plans to protect personal information and prevent breaches, businesses should have response plan to deal with possible breaches. Wisconsin requires businesses to notify persons whose personal information has been compromised in a security breach and the specific information involved. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: Social Security Number; driver's license; financial account, credit card, or debit card number along with any PIN or other access code required to access the account; medical information; or health insurance information. The letter of notice should also recommend measures to take to deal with the breach.

- Organize a response team and designate a team leader to manage the activities.
- Draft contingency plans for dealing with various kinds of breaches, including hacking, lost laptop, etc.
- Investigate breaches immediately.
- Disconnect a compromised computer from the Internet.
- Create a list of who to notify inside and outside of your business in the event of a breach. The latter include the appropriate law enforcement agencies, the persons whose information has been compromised, and the media.
- Draft notification letters and other written communications.
- Consider what outside assistance is needed, e.g., in forensics, media relations, etc.

Procedural and Operational Protective Measures

- Classify information into categories based on importance and confidentiality. Use labels such as "Confidential" and "Sensitive." Identify software, programs, and data files that need special access controls. Employee access should be limited to what he or she needs to do their jobs. No employee should have unlimited access.
- Install software-access control mechanisms. Require a unique, verifiable form of identification, such as a user code, or secret password for each user. Install special access controls, such as a call back procedure, if you allow access through a dial telephone line connection.
- Have your Information Technology (IT) manager change administrative password on a regular basis. A number of free tools are available for this if manual modification is not practical. This password should also be changed during non-business hours.
- Require that passwords consist of a random sequence of at least eight letters, numbers, and special characters. Passwords should be changed at least every three months and not be shared.
- Employee user accounts should not have administrative privileges. This will prevent the installation of any unauthorized software or malicious code that an employee might activate.
- Change security passwords to block access by employees who change jobs, leave, or are fired. The latter become a high risk to your business for revenge or theft.
- Encrypt confidential data stored in computers or transmitted over communication networks. Use National Institute of Standards and Technology (NIST) data encryption standards.
- Design audit trails into your computer applications. Log all access to computer resources with unique user identification. Separate the duties of systems programmers, application programmers, and computer programmers.
- Review automated audit information and control reports to determine if there have been repeated, unsuccessful attempts to log on both from within and outside your facility. Look for unauthorized changes to programs and data files periodically.
- Use monitoring or forensic tools to track the behavior of employees suspected of malicious activities.
- Monitor incoming Internet traffic for signs of security breaches.

- Make backup copies of important business information, i.e., documents, spreadsheets, databases, files, etc. from each computer used in your business. This is necessary because computers die, hard disks fail, employees make mistakes, malicious programs can destroy data, etc. Make backups automatically at least once a week if possible. Test the backups periodically to ensure that they can be read reliably. Make a full backup once a month and store it in a protected place away from your business.
- Delete all information stored in your printers, copiers, and fax machines at least once a week. Use a secure data deletion program that will electronically wipe your hard drives. Simply hitting the delete key will leave some data on the hard drive.
- Be careful in getting outside help with computer security problems. Start with a list of vendors or consultants. Then define the problem, send out a request for quotes, examine each quote, and check the provider's references and history before hiring one.
- If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center (NW3C), at www.ic3.gov. The IC3 website also includes tips to assist you avoiding a variety of Internet frauds.

Protecting Bank Accounts

- Set up dual controls so that each transaction requires the approval of two people.
- Establish a daily limit on how much money can be transferred out of your account.
- Require all transfers be prescheduled by phone or confirmed by a phone call or text message.
- Require that all new payees be verified.
- Check bank balances and scheduled payments at the end of every workday, rather than at the beginning, and contact the bank immediately if anything is amiss. Timely action can halt the completion of a fraudulent transaction because transfers usually aren't made until the next morning. Inquire about your bank's defenses against cyber attacks and review the terms of your banking agreement with regard to responsibilities for fraud losses. Shop around for banks that provide better protections.
- Conduct online business only with a secure browser connection, which is usually indicated by a small lock in the lower right corner of your web browser window. Erase your browser cache, temporary Internet files, cookies, and history after all online sessions. This will prevent this information from being stolen if your system is compromised.

Special Measures for Laptops

Special security measures are needed for laptops to reduce the threat from determined thieves.

- Issue desktops instead of laptops to employees who seldom leave their offices.
- Have employees lock up their laptops when they are left unattended in their offices. Never leave laptops unguarded.

- Have employees carry their laptops in a sports bag or briefcase instead of the manufacturer's bag.
- Do not leave laptops in vehicles.
- Determine if employees need all the data on their laptops to perform their jobs. Remove any data that is not needed.
- Train employees in the need for special measures to protect laptops and their data wherever they may be used.
- Create a loss response team to monitor compliance with laptop and data security measures, investigate losses, assess data needs, and remove data no longer needed.
- Protect data with strong passwords.

Other measures should be considered to protect your business in the event a laptop is lost or stolen.

- Have employees back up their files so they can be recovered if their laptop is lost or stolen.
- Don't store passwords on laptops.
- Encrypt all sensitive information so it cannot be compromised.
- Keep a record of all laptop model and serial numbers and makes so if one is recovered you can prove it is yours.
- Place stickers on the laptops with a phone number to call if one is lost and found by an honest person. But don't put the name of your employee or business on it. That information could be used by criminals to guess passwords or assess the sensitivity of the data stored on the laptop.
- Install hardware, software, or both to aid in recovery of the laptop. After you report the laptop lost or stolen the software enables a monitoring company to track the laptop when the thief logs onto the Internet.

Hardware systems work the same but have a Global Positioning System (GPS) device that can pinpoint its location.

- Install software that will enable you to erase sensitive information when the thief logs onto the Internet.

Use of Social Media

While the use of social media can stimulate innovation, create brand recognition, generate revenue, and improve customer satisfaction, it has inherent risks that can negatively impact business security. Thus, businesses need to develop a social media strategy and a plan to address these risks. Some risk mitigation techniques for business and employee use of social media are listed below.

- Ensure that anti-virus and anti-malware controls are updated daily.
- Use content filtering to restrict or limit access to social media sites.
- Establish policies for the use of mobile devices to access social media. Install appropriate controls on mobile devices.

- Conduct awareness training to inform employees of the risks in using social media.
- Provide employees with clear guidelines regarding what information about the business can be posted.
- Scan the Internet for unauthorized or fraudulent use of the business name or brand.

SHOPLIFTING

Shoplifting can cost your business thousands of dollars each year. Shoplifters may be any age, gender, or economic or ethnic background. There is no "typical" shoplifter. They often work in pairs or groups to divert the clerk's attention while they steal. They often operate when employees are apt to be less alert, e.g., at store opening and closing times, during the lunch and dinner times, and during shift changes. Shoplifters also learn to take advantage of crowded stores during peak hours. Effective prevention begins with an aware and alert staff. The following tips will help prevent shoplifting.

Anti-Theft Devices

- Install security towers at your exits. They will sound an alarm or otherwise indicate when someone takes a tagged item out of the store without paying for it and having the tag deactivated or removed.
- Attach anti-theft tags to your merchandise. Provide cashiers with a means of deactivating or removing the tags when items are paid for.

Display Strategies

- Minimize the shoplifter's access to merchandise without inconveniencing customers.
- Keep display and clothing racks away from entrances and exits to discourage "hit-and-run" thieves.
- Alternate hangers front-to-back to prevent thieves from quickly grabbing bundles of display clothing.
- Keep small and expensive items out of reach or in locked display cases. Have salespeople show only one item at a time from a case.
- Protect merchandise in display cases by keeping the case doors locked and installing laminated glass or clear acrylic plastic in the windows. Use plastic tie-downs or metal chords to secure merchandise on the top of cases.
- Use good locks and laminated or “strong” glass in cases that contain expensive items. This will help prevent smash-and-grab attacks.
- Arrange merchandise neatly to make it easier to detect missing items.
- Take daily or weekly inventories of expensive items.

Educating Employees

Train your salespeople to:

- Watch for people with loose or baggy clothing inappropriate for weather, and people with large bags or other props, such as newspapers, strollers, briefcases, or umbrellas that can easily conceal merchandise.
- Pick up stray receipts around the store.

- Be aware of shoplifter's tactics to confuse and distract you. For example, when working in teams one shoplifter will create a disturbance, e.g., complaining loudly, staging a faint, or knocking over merchandise, to draw attention away from the other who is doing the lifting.
- Be attentive to people in your area. This helps legitimate customers and deters shoplifters. A simple "Can I help you?" or "I'll be with you in a moment" warns shoplifters they are being watched. Keep a close watch on people who seem nervous or refuse assistance.
- Cover their entire area of responsibility, even blind spots.
- Have another salesperson cover your area when you leave the floor, e.g., to check for items in the stockroom.
- Be especially alert at when the store is crowded. Shoplifters often operate when salespeople are busy helping legitimate customers.
- Watch for shoppers walking with short or unnatural steps, which may indicate that they are concealing lifted items.
- Watch customer's eyes. If they are looking at you, they may need assistance or are thinking about shoplifting.

Train cashiers to:

- Check the lower racks of shopping carts, watch for switched labels, look inside items that can also be used as containers for lifted items, e.g., toolboxes, jacket sleeves, waste baskets, etc.
- Check for factory seals on boxed items. And look inside if the boxes are not sealed.
- Staple receipts to the outside of packages.
- Check for and remove or desensitized electronic tags.
- Be familiar with the store prices. This can help prevent price switching.

Have supervisors:

- Keep employees alert by holding periodic review sessions on store shoplifting policies.
- Discourage socializing on the sales floor. A group of employees in one spot usually means inadequate coverage somewhere else.
- Schedule hours so that an adequate number of salespeople are working at all times.
- Watch for customers lingering in one area, loitering near stock rooms or other restricted areas, or wandering aimlessly through the store.
- Watch for customers who consistently shop during the hours when few people are working in the store.
- Watch for customers who visit the store frequently but make only token purchases.
- Be alert for disturbances that distract salespeople and cashiers.

Fitting Room Security

- Keep fitting room doors locked when not in use.
- Install cafe doors to allow staff members to monitor fitting room use.
- Limit the number of items allowed to be taken into the dressing room.

- Post a sign that directs customers to see a salesperson before taking items into a fitting room.
- Issue color-coded tickets and tags to indicate the number of items taken into fitting rooms.
- Use a return rack for unwanted items.
- Post signs in fitting rooms warning against shoplifting.

Preventing Ticket Switching

- Use tamper-proof gummed labels.
- Attach tags with a hard-to-break plastic string.
- Use preprinted, not hand-written, price tags.
- Use concealed multiple price tags.

Protective Measures

- Make the shoplifters feel watched. Elevate the cashier's platform. Install mirrors that enable cashiers and salespeople to see over and around displays. Install one-way glass in offices to enable employees to see into the store without being seen from the floor.
- Install surveillance cameras to cover cash registers, high-value merchandise displays, entrances, loading docks, etc. Use software that can be programmed to create an alarm when suspicious activity occurs. Mount monitors showing live video at main entrances to let shoppers know that they will be under surveillance in the store.
- Post signs warning against shoplifting. Emphasize that you will prosecute. The best way to discourage shoplifters and keep your business from being tagged as an easy mark is to take a get- tough attitude and prosecute on the first offense.
- Encourage checking parcels on entry.
- Require receipts for merchandise returns for cash. Require a photo ID and signature for returns without a receipt. And then just give merchandise-only vouchers.
- Take an inventory of returned merchandise against receipts on a regular basis to catch false returns, i.e., ones without returned merchandise.

Stopping a Shoplifter

If you suspect that someone may be considering lifting something, approach the person and ask, "Can I help you?" or "Can I ring that up for you?" If you suspect someone has lifted and concealed something, keep him or her in sight and notify manager or security personnel immediately. If you are working alone, request the assistance of another worker. Plan a "buddy system" for your own safety and as a witness.

If someone leaves your store without paying for an item, have an employee follow the suspect and get a good description of him or her and any vehicle used, and call 911 to report the crime. Do not have your employee attempt to detain the suspect unless he or she has been trained in apprehension and arrest procedures.

CHECK & CREDIT CARD FRAUD

Bad checks affect everyone in terms of higher consumer costs that must be paid to offset losses, as well as the costs involved in law enforcement and prosecution. There is not completely "safe" method of screening checks, even certified checks can be forged or altered. The best rule is still "KNOW YOUR CUSTOMER." Set up a check cashing and credit card acceptance policy to limit losses. Decide which checks you will accept and set a limit on the amount. The single most important element to cutting losses and providing customer service is EMPLOYEE TRAINING. Make sure employees know and adhere to store policy. The following are guidelines to set up when establishing your policy.

Avoiding Bad Checks

Remember that a check is not legal tender. You are doing the customer a favor by cashing a check. Keep the following in mind:

- Bad checks are most frequently passed on weekends and holidays.
- Persons passing out of state checks are hard to prosecute in Wisconsin.
- Calling a telephone number on a check is not real protection against a forger. The forger may have an accomplice answer the phone. Anyone can get a name from the phone book.
- A bankbook is no proof of funds in the bank.
- A driver's license or credit card alone is not sufficient ID when cashing checks for strangers. Temporary driver’s licenses, social security cards, work permits, voter registration cards, and hunting or fishing licenses are not IDs.
- You have no criminal recourse against the maker or payee on a two-party check.
- The police rely on merchants to report persons passing bad checks. But the police are not a collection agency.

Tips for Cashiers

- Be sure the tended instrument is really a check and not a voucher or merchandise order.
- Never take a postdated check. Make sure the check has the current date.
- Never accept a stale-dated check. Six months is usually the time limit banks will adhere to.
- Never accept a check if the payer states he/she must make a deposit to cover it.
- Never take a check from a person who is drunk or drinking to excess.
- Make sure the check is complete and properly made out. Call your supervisor or the bank if you are in doubt.
- Never accept partial payment on a suspicious check if you contemplate legal action.
- Never accept an altered check or checks with erasures or written over amounts.
- Never take a double endorsed or three-party check.
- Never be afraid to ask for good ID. An honest person does not mind, and you may deter a dishonest one.
- Never let a payer hurry you in the examination of a check or ID. Be on guard when a "fast talker" attempts to cash a check.

- If the payer offers a Wisconsin driver's license for an ID, have him/her take it out and hand it to you. Feel it for bumps on or around the photo, or a slick surface. Check the color and size of photo. Look at the type; if it is typewritten it is probably bogus.
- Compare the description on the ID with the person presenting the check.
- Compare the signature on the ID with the one on the check.
- Compare the address on the ID with the one on the check.
- Make sure the check has the name and location of the bank.
- Make sure the written and numerical amounts match.
- Have the payer sign or endorse the check in your presence. If in doubt, turn the check upside-down and have the endorser sign it on the other end.
- Initial the check so you can identify it later if necessary.
- Get a complete description of the person if there is anything suspicious about the transaction. This can be written on the check.
- Know who in your organization accepted the check.
- Limit check-cashing authority to one or two specially trained cashiers. They will become experts at it.
- Have your employees' initial checks at the time of acceptance.
- Call the NPD immediately after it is determined that the check is not good. Time is of the essence in such situations. Call 911 if the person is still on the premises. Try to delay the person without arousing his/her suspicion and get a good physical description. Study the person’s face and clothing and note any other distinguishing features.
- If the person leaves prior to the arrival of police, get a complete description of his/her vehicle with the license number and direction of travel. But do not expose yourself to any danger.
- If the person is gone by the time, it is determined that the check is not good, call the NPD on its non-emergency number, 886-6000.

Curb Credit Card Crimes
Stolen credit cards or "hot card" losses can be reduced by alertness and proper security measures by you and your employees. When making credit card transactions, cashiers should:

- Request to see a valid ID.
- Check credit card numbers against current "hot sheet" listings.
- Call the card issuer for authorization if you are suspicious about the card.
- Check the card expiration date.
- Compare signature on card with the one on the sales receipt.
- Check that the card has not been altered by "shaving" or "ironing."
- Verify the card before approving a purchase over the floor limit.
- Contact their supervisor if you suspect fraud.
- Keep the card and attempt to stall the customer until security personnel or the police arrive.
- Destroy carbons from credit cards invoices.

Watch out for customers who:

- Chat a lot to distract the clerk or cashier
- Delay purchases until the clerk is distracted or upset
- Hurry the clerk just before closing time
- Purchase a large item such as a TV, and insist on carrying it out rather than having it delivered
- Purchase without regard to size, color, style, or price, or refuse to have alterations which are included in the purchase price
- Purchase several items in the same department, all under the amount of the floor limit or the amount that would require an authorization call to the card issuer