# Protecting Your Business: Crime Prevention

## Risk Control

CNA

Business crime is often seen as victimless because of the perception that most businesses are profitable and insured. For small businesses struggling to survive, crime can often tip the balance from success to failure. When businesses fail, communities may be deprived of goods and services. Without successful small businesses, efforts at regeneration can flounder and employment and investment opportunities may suffer. An effective strategy for tackling crime against business can be an essential tool if the economy is to flourish and communities are to prosper.

There are numerous simple, low-cost crime prevention measures that small businesses can implement to help reduce the effect of crime. This guide was developed to provide information and concepts that can be used to help identify areas with exposure to loss and measures to reduce the potential for loss. This guide is not intended to be an all-inclusive summary of all hazards and controls.

The following sections are included in this document:

- Pre-employment Screening
- Employee Theft Prevention
- Credit Card and Check Fraud
- Shoplifting
- Violence in the Workplace
- Burglary
- Robbery
- Premises Liability

## Pre-employment Screening

Employee selection, perhaps more than any other process in an organization, can have the power to change a company's destiny. The proper time spent in the selection and training process allows employers to hire the best possible employees.

Employers should establish a policy regarding when and under what circumstances pre-employment background checks are to be performed. The amount of background investigation performed on an applicant should be proportional to the degree of risk presented by the position being filled.

Because of the potential of severe consequences to a business from negligently hiring an employee, a careful, thorough investigation into the background and fitness of a prospective employee is essential to the well-being of the business. Negligent hiring liability is a basis for recovery against employers for the wrongful and even criminal actions of employees against third parties. This can occur when the offending employee is hired without an adequate background investigation and when such an investigation would have indicated the applicant was a potential risk.

Pre-employment screening programs begin with an employment application form that can obtain information necessary for a thorough background investigation. The job application form provides the first opportunity to gather the prospective employee's information and can help to make the screening process much easier.

## Job Application

- The application form should be developed with the assistance of legal counsel.
- The form should declare that all false statements are grounds for rejection or immediate termination. Establish a policy on the actions to be taken when such false statements are discovered.
- The application form should be signed by the applicant.
- A release and authorization form, signed by the applicant, will allow for verification of all information on the application form. This form should also provide authorization for obtaining criminal and credit history checks.

The application should include, but not be limited to, the following:

- **Biographical Information** — Name, address, driver's license and Social Security number, as well as previous addresses and whether the applicant has worked under other names and/or Social Security numbers.
- **Employment Desired** — Position and availability.
- **Education** — Names and addresses of schools, certifications, dates attended and certifications received.
- **Employment History** — Names of former employers, dates of service(s), job duties, supervisor(s) and reason(s) for leaving.
- **References** — Name, telephone numbers and relationship to potential employee.

# Pre-employment Screening Methods

Employers have numerous options available to screen applicants, such as resumes, job applications, reference checks, interviews and background checks. While some may be time-consuming and expensive, many are straightforward and cost-effective. The failure to investigate properly could cause severe consequences to a business.

## What Should Be Included in a Background Check?

- Driving records (MVRs)
- Vehicle registration
- Credit records
- Criminal records
- Social Security number
- Education records
- State licensing records
- Past employment — work history
- Military records
- Reference checks
- Bankruptcy

Employers are not exposed to liability simply because they failed to check an applicant's background. But, if such a check would have revealed information indicating the undesirability of the applicant, this failure to obtain information may be considered negligence.

# Employee Theft Prevention

Small businesses, especially those that do not conduct regular audits, should be aware of factors that can contribute to small business fraud. For example:

- **Inadequate Employee Pre-screening** — Oftentimes, small businesses do not spend the money to check work references or records of potential hires.
- **Limited Controls** — Small businesses frequently have insufficient personnel to adapt adequate controls, including internal and external audits and fraud hotlines. In addition, some of the very things that can make a small organization a pleasant place to work, e.g., flexible work hours, employees not required to clock in or use a security badge to enter and exit the building, can also enable thieves to succeed.

Three major categories of occupational fraud to consider are:

- **Asset Misappropriations** — These schemes involve the theft or misuse of an organization's assets by such means as skimming revenues, stealing inventory or committing payroll fraud.
- **Corruption** — This occurs when fraudsters wrongfully use their influence in business transactions to procure some benefit for themselves or another person. One of the most common is accepting kickbacks or engaging in conflicts of interest.
- **Fraudulent Financial Statements** — These generally involve falsification of an organization's financial statements by overstating revenues or understating liabilities or expenses.

## Preventing Employee Theft

- Establish a written policy that outlines employee responsibilities, standards of honesty, general security procedures and consequences if not followed. Ensure new employees read the policy, understand it and sign it as a condition of employment.
- Follow strict hiring practices. Verify all information and contact all references listed on an application.
- Keep and maintain accurate records on cash flow, inventory, equipment and supplies. Have it reviewed regularly by someone other than the person responsible for maintaining it.
- Limit access to keys, the safe, computerized records and alarm codes. Engrave "DO NOT DUPLICATE" on store keys. Change locks and access codes when an employee is terminated.
- If internal theft is discovered, take action quickly. Contact your local law enforcement agency and be sure to send a message to your employees that theft will not be tolerated.
- Reward employees for uncovering security problems and good performance.

# Credit Card and Check Fraud

## Credit Card Fraud

According to a report published by the Department of the Treasury, United States Secret Service, credit and charge card fraud costs cardholders and issuers hundreds of millions of dollars each year. While theft is the most obvious form of fraud, it can occur in other ways. Employees should be prepared and trained to identify credit card fraud.

Types of credit card fraud:

- Stolen credit cards
- Identity fraud
- Altered credit cards
- Counterfeit cards

**Training and Prevention**

- Train employees to follow each credit card company's authorization procedures.
- Be skeptical of a customer with only one credit card and one piece of identification.
- Be aware of the customer who makes several small purchases by check or credit card that fall under the amount for manager approval.
- Be aware of items being purchased that could be easily fenced for cash, e.g., televisions, stereos, cameras and other portable items.
- If suspicious of the purchaser, make a note of appearance, companions, any vehicle used and identification presented. Call the local police department.
- Look for "ghost" numbers or letters. Many times criminals will change the numbers and/or name on a stolen card. To do this, the offender may either melt the original name and numbers off or file them off. Both of these processes can leave faint imprints of the original characters.
- Examine the signature strip on the credit card. A criminal may cover the real card owner's signature with correction fluid and sign it on the new strip.
- Check to see if the signature on the card compares favorably with the signature on the sales slip.

## Check Fraud

According to the Check Fraud Center (www.ckfraud.org), check fraud is one of the largest challenges facing businesses and financial institutions today. With the advancement of computer technology, it is increasingly easy for criminals, either independently or in organized gangs, to manipulate checks in such a way as to deceive innocent victims expecting value in exchange for their money.

**Types of Check Fraud**

- **Forgery** — For a business, forgery typically takes place when an employee issues a check without proper authorization. Criminals, using false personal identification, can steal a check, endorse it and present it for payment at a retail location or at a bank teller window.
- **Counterfeiting and Alteration** — Counterfeiting can either mean wholly fabricating a check – using readily available desktop publishing equipment consisting of a personal computer, scanner, sophisticated software and high-grade laser printer – or simply duplicating a check with advanced color photocopiers. Alteration primarily refers to using chemicals and solvents such as acetone, brake fluid and bleach to remove or modify handwriting and information on the check. When performed on specific locations on the check, such as the payee's name or amount, it is called spot alteration. When an attempt to erase information from the entire check is made, it is called check washing.
- **Paperhanging** — This problem primarily has to do with purposely writing checks on closed accounts (their own or others) as well as reordering checks on closed accounts (their own or others).
- **Check Kiting** — Check kiting is opening accounts at two or more institutions and using "the float time" of available funds to create fraudulent balances. This fraud has become easier in recent years due to new regulations requiring banks to make funds available sooner, combined with increasingly competitive banking practices.

Many fraudulent checks are visibly phony. By paying close attention to a check's appearance, one can often detect a possible bad check before accepting it as payment. One or more of the following telltale signs may represent a phony check:

- No perforation on check edges
- Apparently altered writing or erasures
- Water spots or alterations of check's color or graphic background
- Numbered under 500 (new account)
- Post-dated
- Glossy rather than dull finish of magnetic ink
- Signature does not match imprinted name and ID

Protect the business against possible losses by requiring management approval of the check or asking for an alternative form of payment.

# Shoplifting

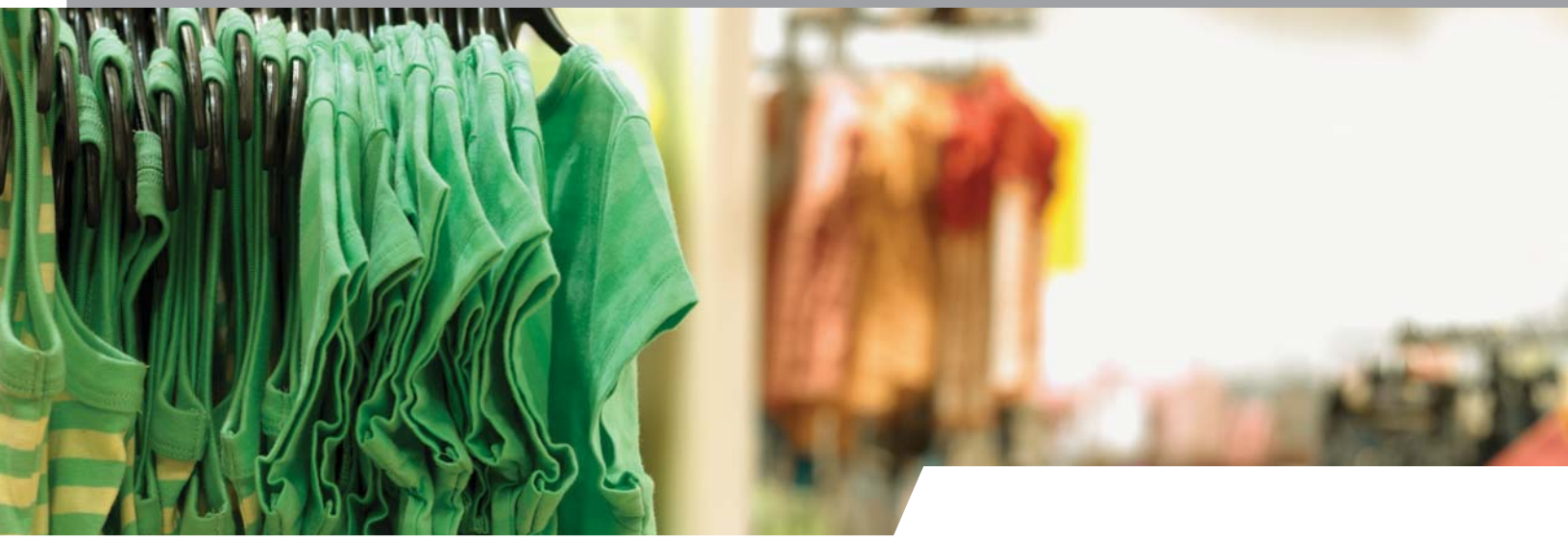
Petty thievery may not seem like a major crime to the casual crook who pockets a ballpoint pen here and a pocket calculator there. But to the small business fighting for survival, it can be devastating. Shoplifting is defined as the act of stealing goods that are on display in a store. According to the University of Florida's *2003 National Retail Security Survey*, simple steps may help prevent losses from shoplifting.

## Profile of a Shoplifter

What do shoplifters look like? Shoplifters are male or female, any race or color, and there are no age limitations. Anyone who deliberately takes merchandise from a store without paying for it is a shoplifter, whether the theft is large or small, premeditated or impulsive. Fortunately for business people, most shoplifters are amateurs. To the wary eye, they are not difficult to spot and, with the right kind of handling, may never try petty thievery again.

## Shoplifting Prevention

- Train employees how to reduce opportunities for shoplifting and how to apprehend shoplifters. Work with law enforcement to teach employees what actions may signal shoplifting.
- Keep the store neat and orderly. Use mirrors to eliminate "blind spots" in corners that might hide shoplifters. Merchandise should be kept away from store exits to prevent grab-and-run situations.
- Keep displays full and orderly so employees can see at a glance if something is missing. Keep expensive merchandise in locked cases. Limit the number of items employees remove at any one time for customers to examine.
- Design the exits of the business so all persons must pass by security personnel or store employees. You may want to use an electronic article surveillance system or other inventory control devices.
- The cash register should be inaccessible to customers, locked and monitored at all times. Place it near the front of the store so employees can also monitor customers coming and going.
- Dressing rooms and rest rooms should be watched at all times. Keep dressing rooms locked and limit the number of items a customer can bring into the room.



# Violence in the Workplace

Violence in the workplace has received considerable attention in the press and among safety and health professionals. Much of the visibility given to this issue has been from reporting of data by the National Institute for Occupational Safety and Health (NIOSH) regarding the magnitude of this problem in U.S. workplaces.

According to the report, *Violence in the Workplace*, DHHS (NIOSH) Publication No. 96-100, the spectrum of workplace violence ranges from offensive language to homicide. A definition of workplace violence is as follows: *violent acts, including physical assaults and threats of assault, directed toward persons at work or on duty.*

Violence is a substantial contributor to death and injury on the job. NIOSH data indicates that homicide has become the second leading cause of occupational injury death, exceeded only by motor vehicle-related deaths. Workplace violence is not distributed randomly across all workplaces, but is clustered in particular occupational settings. More than half (56%) of workplace homicides occurred in retail trade and service industries. Homicide is the leading cause of death in these industries as well as in finance, insurance and real estate. 85% of nonfatal assaults in the workplace occur in service and retail trade industries.

Long-term efforts to reduce the level of violence in U.S. society must address a variety of social issues, such as education, poverty and environmental justice. However, short-term efforts must address the pervasive nature of violence in our society and the need to protect workers. Workplace violence needs to be addressed not only as a social issue but as a serious occupational safety issue.

Following are prevention strategies that businesses can implement to help reduce workplace violence:

## Environmental Designs

- Locked drop safes, which carry small amounts of cash, and posting signs that limited cash is available.
- Physical separation of workers from customers, clients and the general public through the use of bullet-resistant barriers or enclosures.
- Proper lighting to increase visibility.
- Access to and egress from the workplace.
- Installation of security devices.
- Available personal protective equipment.

## Administrative Controls

- Staffing plans and patterns, such as escorting patients and prohibiting unsupervised movement and, if appropriate, increasing the number of staff on duty in any number of services and retail settings. In addition, the use of security guards or receptionists to screen persons entering the workplace can help to control access to actual work areas.
- Work practices, such as staffing patterns, during the opening and closing of establishments and during money drops and pickups, taking out garbage, disposal of grease, storing food or other items in external storage areas and transporting of store money.
- Policies and procedures for assessing and reporting threats.

## Behavioral Strategies

- Training employees in nonviolent response and conflict resolution.
- Training employees on hazards associated with specific tasks or work sites.

# Burglary

Burglary is any unlawful entry to commit a felony or a theft, even if no force is used to gain entrance.

According to the article "Curtailing Crime – Inside and Out" by the U.S. Small Business Administration: "Retailers whose stores have been broken into know that burglaries are costly. What these business owners may not be aware of is that the number of burglaries has doubled in the past several years and, therefore, they may be two, three or four time losers if the trend is not reversed. Moreover, few burglars are caught; almost 80% of burglaries go unsolved. Arrest and prosecution are difficult because of a lack of witnesses or evidence to identify the criminal."

Prevention, therefore, must start with the merchant — you. Use a combination of measures to protect your store from burglars such as:

- Suitable locks
- An appropriate alarm system
- Adequate indoor and outside lighting

## Locks

Be sure to use the right kind of lock on doors. In addition to being an obstacle to unwanted entry, a strong lock requires a burglar to use force to get into the store. Most experts on locks agree that the pin-tumbler cylinder lock provides the best security because it can have from three to seven pins. Locksmiths caution that a burglar can pick a lock with less than five pins.

Deadbolt locks (bolts that are moved by turning the knob or key without action of a spring) can be used. When using a double cylinder deadbolt lock, the door cannot be opened without a key on either side. Using this type of lock on a glass door ensures there is no handle for a burglar to reach by merely breaking the glass.

## Key Control

To keep keys from falling into the hands of burglars, issue as few keys as possible and keep a record of those issued. Exercise the same care with keys as you would with a thousand-dollar bill:

- Avoid key duplication.
- Keep records on key distribution up to date to be aware of what keys have been issued and to whom they have been issued.
- Whenever a key is lost or an employee leaves the firm without turning in his or her key, re-key the locks.
- Have one key and lock for outside doors and a different key and lock for the office.
- Have a code for each key so that it does not have to be visibly tagged and allow only those authorized to know the specific lock that key fits.
- Take a periodic inventory of keys.

## Alarm Systems

Burglar alarm systems are intended to detect the entry or attempted entry of intruders into a protected facility and signal their presence to others, either locally or at a remote location, initiating certain procedures intended to prevent or minimize loss.

Underwriters Laboratories Inc. (UL) provides the classification system for business burglar alarm systems. UL classifies burglar alarm systems by type or principle of operation as central station, proprietary, limited mercantile or bank.

**Central Station**
A central station system is one in which the operation of electrical protection circuits and devices are signaled automatically, recorded, maintained and supervised from a central station having trained operators on duty at all times.

**Proprietary**
A proprietary burglar alarm system is one in which alarm initiating circuits and devices are installed at a property and are connected directly or indirectly to constantly monitored receiving equipment at a central supervising station. The central supervising station is operated by personnel responsible to the owner of the protected property.

**Limited Mercantile**
A mercantile alarm system is one in which the protective circuits and devices of a mercantile premises, safe, vault, ATM or night depository are connected to an enclosed and tamper-protected alarm-sounding device and may not be connected to a remote location. The device is attached to the outside of the building on the premises.

**Bank**
A bank alarm system is one in which the protective circuits and devices of a bank safe, vault, ATM or night depository are connected to an enclosed and tamper-protected alarm-sounding device attached to the outside or the inside of the building in which the protected item is located — generally used for banking institutions.

## Lighting

This is an important and often underestimated aspect of security for all types of businesses. On average, there are 3,000 hours of darkness a year. It is perhaps no surprise that most burglaries against commercial premises occur during the hours of darkness.

Properly installed and maintained interior and exterior lighting can help guard against unnoticed entry.

- **Exterior** — Lighting should be provided within approximately 20 feet of the main entrance. Dark and obscure areas of the property (e.g., back and side doors, windows and other points of access) should be lighted, if vulnerable, and not visible from streets or highways.
- **Interior** — Lighting should be provided in areas easily visible from outside the building.
- **Exterior Yard Storage** — Adequate area lighting should be provided when materials, equipment or vehicles are stored on the property.

## Closed-circuit Television (CCTV)

Closed-circuit television (CCTV) systems are widely used in commercial settings as a safety and security system. CCTV systems have found applications in:

- Lobbies of buildings to identify visitors requesting entry
- Retail establishments to detect shoplifting and employee theft
- Parking lots to monitor potential criminal activity
- Schools, as a deterrent to vandalism
- Galleries and museums to provide surveillance of valuable paintings and art treasures
- Automatic teller machines or electronic cash registers to record transactions and, combined with video motion detectors, to detect and record unauthorized intrusions
- Hospitals where CCTV can be used to monitor intensive care patients
- Research and development labs
- 24-hour recordings of experiments
- Public-access areas to help personnel watch for emergencies requiring immediate attention, such as accidents in highway tunnels

CCTV is a television transmission system in which live or prerecorded signals are sent over a closed loop to a finite and predetermined group of receivers, either via coaxial cable or as scrambled radio waves that are unscrambled at the point of reception or the television monitors. The camera, which is the device that captures and transmits a picture of the scene, is usually located remotely from the monitor. The cameras need to be capable of operating or transmitting a picture with the level of lighting provided. The monitor can be located at a console in another room, or even in another building, and allows security personnel to remotely view the scene.

Recent technological innovations have decreased the cost of CCTV systems and greatly increased their usefulness. The number of different applications for CCTV systems is as varied as the environments in which they are used.

**Security Surveillance**
The traditional role of CCTV in security has been to expand the surveillance capabilities of security personnel without a corresponding increase in manpower costs.

**Access-Control**
Among the uses of CCTV in access-control are to remotely identify visitors requesting entry, to verify the identity of employees entering a facility and to determine who wants to get into or leave a restricted area.

**Alarm Detection and Monitoring**
A video motion detector functions as part of an intrusion detection system that signals an alarm when motion occurs on a monitor's screen. Video motion detection is not meant to replace an intrusion detection system but, rather, to enhance it providing secondary detection and backup to the primary system.

# Robbery

Robbery is defined as stealing or taking anything of value by force, violence or threat.

The criminal, in selecting a store to rob, looks for places that are isolated, easy to enter and exit, and where there would be the least effort to overcome the resistance of cashiers. The most vulnerable robbery targets are convenience stores, gasoline stations, drive-ins and liquor stores on or near a major thoroughfare, staffed by a single clerk and operating late at night with the day's receipts still on hand.

Although the dollar loss from robbery is somewhat small — approximately $525 million in 2004, as estimated in *Crime in the United States 2004 (Uniform Crime Reports)*, published by the Federal Bureau of Investigation (FBI) — the impact of this crime cannot be measured in terms of economic loss alone. While the target of a robbery is money or property, many victims of robbery suffer serious personal injury.

Robbery doesn't occur as often as other crimes against businesses, but the potential for loss can be much greater from a single incident. In addition, robbery involves force or threat of force and can result in serious injury or death. Following are strategies that could help to thwart would-be robbers:

- Greet every person who enters the business in a friendly manner. Personal contact can discourage a would-be criminal.
- Keep windows clear of displays or signs and make sure your business is well-lighted. Check the layout of your store, eliminating any blind spots that may hide a robbery in progress.
- Provide information about your security systems to employees only on a need-to-know basis. Instruct your employees to report any suspicious activity or person immediately and write down the information for future reference.
- Place cash registers in the front section of the store. This increases the chances of someone spotting a robbery in progress and reporting it to the police.
- Keep small amounts of cash in the register to reduce losses. Use a drop safe into which large bills and excess cash are dropped by employees and cannot be retrieved by them. Post signs alerting would-be robbers of this procedure.
- Make bank deposits often and during business hours. Don't establish a pattern; take different routes at different times during the day. Ask a police officer to escort you to the bank whenever possible.
- Ask local law enforcement what to do in case you are robbed. Make sure your address is visible so emergency vehicles can easily find your business.
- Do not release personal information to strangers.
- Keep purses and personal valuables locked in desks or lockers.
- Install a robbery alarm.
- Place a surveillance camera behind the cash register facing the front counter. Replace videotapes regularly.
- Don't use marked "moneybags" that make it obvious to would-be robbers you are carrying money for deposit.
- Place excess money in a safe or deposit it as soon as possible.
- Cooperate with the robber for your own safety and the safety of others.

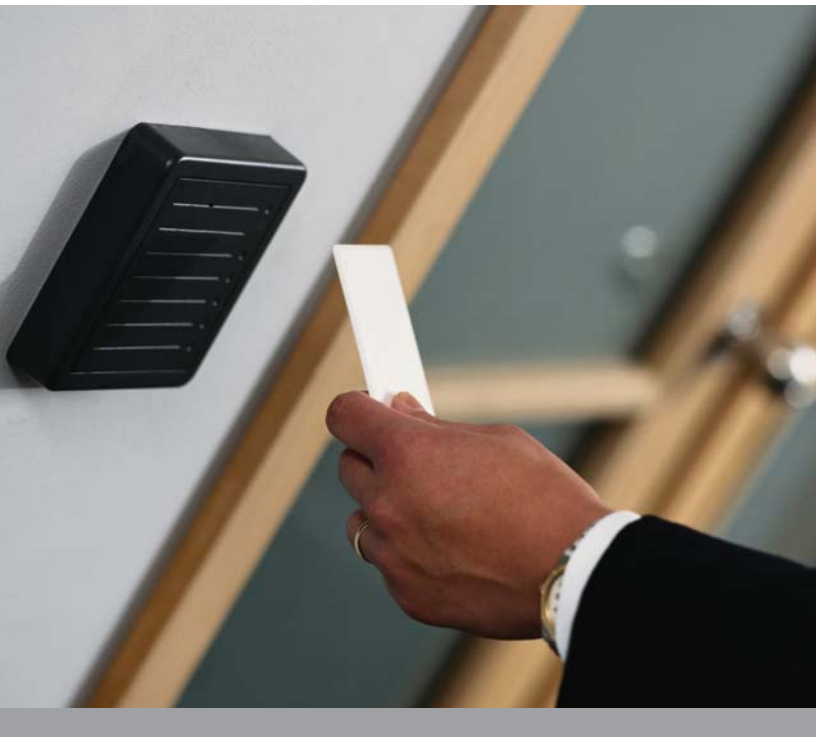
If confronted by a robber, cooperate. Merchandise and cash can always be replaced — people can't!

# Premises Liability

## Premises Security Liability

Premises security liability is the civil liability of property owners for the foreseeable criminal acts of third persons. It arises when a property owner or manager fails to provide a reasonably safe environment and, as a result, someone is victimized by the criminal conduct of another person. Usually, the assailant is known neither to the victim nor the property owner and is not apprehended.

Premises security liability is also referred to as inadequate security liability and includes negligent hiring liability. Except in instances where intentional misconduct occurs, such as for false arrest or excessive use of force, premises security claims are tort claims in negligence and arise from such actions as an inadequate number of security personnel, poor lighting in parking areas, faulty locks, negligent hiring of personnel, inadequate maintenance of security records and failure to repair or maintain security equipment.



## Access-Control Systems

Who is in your business on a daily basis? To increase protection of your personnel and property, consider an access-control system. Access-control systems are utilized to restrict access to portions of the operations and valuable personal property. The access-control system is designed to screen or identify individuals prior to allowing entry. These can range from push-button locks to card-access systems integrated with CCTV. Following are examples of access-control systems:

- **Bar Code** — Not widely used because the encoding security is low and can be easily damaged.
- **Card Technologies** — Card encoding technology.
- **Hollerith** — Oldest access system. Holes are punched into a card and passed through light or brushes with an electric contact. Low security.
- **Infrared** — Data is stored on a card by means of a bar code and read by passing infrared light through the card.
- **Multiple Portal Systems** — Part of a large network of readers to a central processing unit used to regulate multiple entry points.
- **Magnetic Stripe** — Most common system in use. Similar to credit cards and ATM cards, they use a magnetic stripe to allow information to pass into the access reader.
- **Optical Storage** — Information on these cards is generally encrypted. Access passwords are needed and these systems have a high initial cost.
- **Proximity** — Becoming the most popular. Cards only need pass near the reader operating from 2 – 12 inches.
- **Stand-Alone Systems** — Control access to a single point.

## Guard Service

On-premises watch service is a suitable means of burglary protection; however, it is not always economically practical. The presence of guards may be considered in determining the appropriate level of protection. To be considered standard, the following guidelines should be met:

1. Watchmen should cover all important areas, including yard storage, detached buildings, loaded trailers, etc. Key stations should be provided to assure proper coverage.
2. Rounds should be made hourly and be supervised by supervisory initiating devices, such as the key stations noted above or other electronic means. There is value in varying the route of the tour during the course of the day.
3. Watchmen should be responsible only for plant security functions; they should not perform maintenance or other functions.

Watchmen should be well-trained and be provided a means by which they can quickly notify police or other authorities. Written training manuals and procedures help ensure consistency when there is turnover or additions to the guard force.

## Design and Layout

Beginning with the exterior portion of the facility, trees, shrubs and trash dumpsters should not enable intrusion into the facility by providing hiding spaces for a would-be burglar. If present, these items should be kept away from the building to reduce the possibility of climbing onto rooftops for additional access areas.

The interior of the building and occupancy should be designed to minimize or eliminate dark or remote hiding areas for a criminal.

All elevators and stairwell lobbies should provide see-through enclosures or otherwise be arranged so that criminals cannot hide easily.

Exterior and interior lighting should be adequate. Outdoor lighting is another way to shield the store from crime. Darkness conceals the criminal and gives him or her time to work. Burglars can be defeated by floodlighting all around the outside of the store. Indoor lighting is also important. When a store is lighted inside, police officers can see people in the store or notice the disorder that criminals usually cause. When the store is dark, the criminal can see the police approaching, but the police can't see the burglar.

**Doors and Windows**
These are perhaps the most frequent points of entry for the burglar. Windows and doors at the rear of premises may be particularly vulnerable because they are often out of sight of the casual observer.

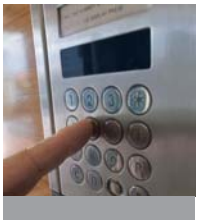
Windows — Windows that are easily reached from the ground or adjacent structures that do not front main roads should be blocked or protected. Protection, as permitted by the governing building and fire codes, should be in the form of bars or screens. At a minimum, all movable windows must have locking mechanisms. Common cam locks found on most windows are acceptable. Windows should have secure locks and burglar-resistant glass.

Doors — All exterior doors should have a metal facing or solid metal construction. The doorframe should also be of substantial construction and be securely mounted to the structure. A heavy deadbolt lock should be provided, with a bolt that extends at least one inch into the frame. At closing, all overhead dock doors should be padlocked through door tracks or their equivalent.

**Heavy Window Screens**
Heavy metal window screens or grating are an inexpensive way to protect show windows. Store them during business hours and, at closing time, put the screens up and lock them in place.

**Burglar-Resistant Glass**
When used in exterior doors, windows, display windows and interior showcases, burglar-resistant glass can deter burglars. It has high tensile strength that allows it to take considerable beating. This glass is a laminated sandwich with a sheet of invisible plastic compressed between two sheets of glass. It mounts like ordinary plate glass and is clear, tinted or opaque.

**Visitors and Tours**
The nature and size of the business will determine the need to control visitor access to all or portions of the premises. At potential risk are proprietary information, data, sensitive equipment and areas where cleanliness is crucial (e.g., laboratories). Tours create unique opportunities for the criminal mind as businesses open their doors to the general public as a good will gesture. Access during tours and to visitors should be limited and controlled. Clear and visible signs in your controlled areas and in your reception area should be provided. A written policy can be developed to provide internal controls and should be easily understood by employees and visitors and uniformly enforced.



**Let us help you create a safer environment today.**

To learn more about how CNA Risk Control can help you manage risk, increase efficiencies and be more productive, call us toll-free at 866-262-0540.

Or, visit the CNA Risk Control Web site at **www.cna.com/riskcontrol**

**To discover the broad range of insurance products available from CNA, contact your independent agent or broker or visit www.cna.com**

CNA


EG SB CP 033106