Bomb, Chemical and Biological Incidents

General Indicators

It is extremely difficult to prepare for and prevent acts of extortion, politically motivated violence or criminal attack due to the covert nature of these activities, however there are a number of indicators that often precede these attacks, regardless of the type of threat or the type of target. These include:

- Surveillance – photography or videotaping.
- Loitering – access to secure or even unsecured areas by unknown or unidentified persons with no reasonable excuse.
- Information requests – requests for plans, blueprints, or engineering specifications for buildings by those who have no official reason to have them.
- Inappropriate clothing – people wearing inappropriate clothing relative to the weather (eg. excessive clothing worn on warm days).
- Multiple indicators – it may be difficult to accurately identify potential terrorist behaviour on the basis of a single indicator. Multiple indicators, however, should arouse considerable suspicion and caution.

Bomb incidents

How to respond to a bomb incident

You should use the following guidelines when dealing with any suspicious item believed to be an explosive:

- Turn off all radio frequency emitting electronic equipment. Radios, pagers, and mobile phones may cause an explosive device to detonate. Use traditional landline telephones to call authorities. If receiving a call regarding a possible bomb threat, leave the land line open and off the hook for later investigation.
- Open any available windows and doors to dissipate explosive energy and mitigate potential damage.
- If a suspicious package or device is found, do not touch it. Immediately evacuate the area and have all people move as far as is possible away from the suspicious package or device.
- If you can see the suspicious package or device, it can see you. Evacuate to a position of safety where you cannot see the device. This will greatly reduce the likelihood of you being injured if it explodes.

If you are in a building or structure, particularly a high-rise building that is a target of terrorist activity, consider the following:

- During the initial attack, you should seek cover under desks or tables. If these items are not readily available, move against an interior wall and protect your head with your arms. Move away from windows and balconies.
- If you are able, immediately evacuate the area and move to a safe location.
- During evacuation procedures, immediately move away from the targeted location and seek shelter inside a secure area. Glass windows and other building materials may be dislodged and may fall outwards several hundred metres.
- If you are outdoors near the targeted location during the initial attack, duck behind an item that will provide you cover, such as a tree or doorway, and get down as low as possible. After the initial attack, move to a safe area away from the targeted location. Stay out of damaged buildings.
- Consider the possibility that additional attacks or secondary explosions may occur.

Chemical incidents

Chemical agents are a means by which terrorist groups may conduct attacks against urban populations. Some examples of chemical agents include:

- Nerve agents: Man made, extremely toxic.
- Choking agents: Gases that cause immediate coughing and choking.
- Blister agents: These are usually liquids and evaporate slowly. An example is mustard gas. Symptoms include reddening of the skin and blistering.
- Blood agents: These are inhaled. An example is hydrogen cyanide. Symptoms include a flushed face with red lips, frothing at the mouth, vomiting, unconsciousness, and death.

Chemical agents enter the body through any one or more means by:

- Inhalation – Breathed in.
- Ingestion – Swallowed. Normally via food or water source.
- Absorption – Penetration of skin or eyes.
- Injection – Physically injected into person or transferred by explosive fragmentation.

During a chemical terrorist attack, the best place to be is upwind and on high ground far from the dissemination location. Changing weather conditions may require personnel to be moved quickly from one location to another position of safety.

Chemical incidents (indicators)

- Dead animals/fish – Numerous animals dead in the same area.
- Blisters/rashes – Numerous individuals experiencing unexplained water-like blisters, weals (like bee stings) and/or rashes.
- Mass casualties – Health problems including nausea, disorientation, difficulty in breathing, convulsions and death.
- Patterns of casualties – Casualties will likely be distributed downwind, or if indoors, by the ventilation system.
- Unusual liquid droplets – A number of surfaces exhibit oily droplets/film. Water surfaces may also have an oily film on the surface.
- Dead/withered vegetation – Trees, bushes, food crops and/or lawns that are dead, discoloured or withered, without drought conditions.
- Unexplained odours – Smells ranging from fruity to flowery, sharp/pungent, or garlic/horseradish like bitter almonds. All smells will be completely out of character for the surroundings.
- Low-lying clouds – Unusual low-lying cloud and fog-like conditions.

Biological Incidents

There are two basic forms of biological agents. They are micro-organisms and toxins. These agents comprise living organisms. Examples of bacteria are anthrax and pneumonic plague. An example of a virus is Ebola. Toxins are poisonous substances produced by plants or animals, and include examples such as botulism and ricin. Toxins and bacteria, such as anthrax, are not contagious. However, viruses such as Ebola are contagious and may be spread from person to person.

Characteristics of biological agents include the following:

- No immediate effect. The symptoms take time to appear, from hours/weeks.
- They must be inhaled or ingested. They do not penetrate unbroken skin.
- They are adversely affected by weather conditions such as sunlight. Therefore, they are more likely to be used at night or in enclosed areas.
- Likely to be spread through the use of aerosols.
- Symptoms include flu-like symptoms.

Biological agents enter the body through any one or more means by:

- Inhalation – Breathed in.
- Ingestion – Swallowed. Normally via food or water source.
- Absorption – Penetration of skin or eyes.
- Injection – Physically injected into person or transferred by explosive fragmentation.

There are no characteristic or immediate signatures of the release of biological agents as they are usually colourless and odourless. A biological incident can therefore only be determined on the basis of its effects upon the surrounding area, and generally after a period of time.

Biological incidents (indicators)

Unusual number of sick and dying – Casualties may occur minutes to hours to days or weeks after an incident has occurred. The time required before symptoms are observed is dependent on the agent used.

Unscheduled and unusual spray – Especially outdoors during periods of darkness.

Abandoned spray devices – Devices will have no distinct odours.

How to respond to a chemical or biological incident

Biological and chemical agents may be disseminated in a variety of fashions, including the use of letters or packages containing these agents. If you receive a letter or package that you suspect is contaminated, do the following:

- Do not handle further. Don't shake/bump it.
- Isolate the package or mail.
- Remain where you are.
- Isolate yourself and all others who came into contact with the suspicious item.
- Do not show it to any further people including your supervisor. You need to minimise the amount of persons who have contact with the item.
- Shut down the air conditioning or ventilation system or contact via landline someone in the building who can.
- Don't open, smell, taste or touch it. This includes your clothing.
- Ensure all persons who handled the package wash their hands with soap and water.
- Do not brush your clothing.
- Remove clothing and place it in a plastic bag as soon as possible (removing of clothing can remove about 80% of the contaminant).
- Shower with soap and water. Do not use bleach or other disinfectants.
- Make a list of all the people who had contact with the substance or package and give it to the investigating authorities.

This advice still applies if the agent is disseminated by other means – for example, through a ventilation system or some other dispersal method.

Armed Robbery – Prevention and Response

You should develop appropriate strategies around how cash is handled and sensible business precautions and procedures to reduce the risk of armed robbery to your business. You should also know what to do if your business becomes a victim of armed robbery.

Cash handling

- Do not keep large amounts of cash on hand and advertise the fact that minimum cash is held on the premises.
- Bank regularly but vary the times of banking and routes taken to the bank. Use two staff members for banking where possible. Larger businesses may consider security pickup of cash.
- Don't use a bank bag, use a less conspicuous bag.
- Remind staff to be on the alert whilst carrying cash.
- Cash should never be counted in view of the public and never leave cash lying around.
- Never talk in public about cash handling procedures.

How to reduce the risk of armed robbery

- Be aware of any suspicious activity near any business. Note the descriptions of any suspicious vehicles and/or persons and inform the police immediately.
- Ensure all doors and windows at the rear of your premises are secured with deadlocks, key locks and/or bars.
- Electronic beepers or other devices should be installed to indicate when people are entering and leaving your premises.
- Shop frontage should be uncluttered providing a clear view to the street. If possible, place your service area in clear view of the street frontage. Have open glass store fronts where possible.
- Ensure you have adequate exterior and interior lighting.
- Consider a silent alarm that is connected to a security company and can be activated from near your cash drawer or register.
- Consider the installation of a security camera that can capture good quality images of the offender/s committing the armed robbery. Ensure that you have a high quality data storage system which has not been reused to the extent that the quality is affected.
- Ensure security camera has unobscured vision of the counter area and that the camera is angled at the right position for face height.
- Consider installing a video screen displaying footage of customers during service. Ensure the screen is in view of customers as this may deter illegal activity.
- Train staff in downloading CCTV footage so that Police have access immediately.

- Ensure that measurement sticks on doors are accurately placed at the right height so that offender can be appropriately measured.
- Have rough height guides in store, e.g. know the height of magazine racks etc. so that comparison can be made to identify a correct height for the offender.
- Ensure that staff are given proper instructions by management to give over all that is requested of them by the armed robber. Instil the mentality that staff safety is paramount.
- Ensure that you have enough insurance to cover any potential losses and inform staff that insurance will cover losses. Some staff members may be concerned about the consequences of handing over money.

If you are a victim of an armed robbery

- Consider your safety at all times. Obey the offender's instructions, but do only what you are told and nothing more. Do not volunteer any information.
- All armed offenders must be treated as dangerous. Some may be under the influence of drugs or alcohol and may react in an unpredictable way.
- Try to remain calm. It can reduce the chance of the offender becoming violent and may enhance your attention to detail.
- Keep your distance from the offender. When asked to hand over the money, place it on the counter and take a step back.
- Keep your hands in sight at all times. If you need to move your hands out of the offender's sight, ask for permission and await approval.
- Be deliberate in your actions. If you are ordered to hand money to the offender, start with lower denomination notes.
- Stay out of danger if you are not directly involved and if you can leave the building safely, do so and then raise the alarm.
- Phone the Police emergency number 000 if you or some other responsible member of your staff is able to do so without danger. If possible keep the line open.
- Alarms should be activated if it is safe to do so. If there is any danger in activating the alarm wait until the threat has gone.

What to do after an armed robbery

- When offender leaves, do not pursue them, use this opportunity to make as many observations as you can including direction and method of departure.
- Phone police first on 000 and management second.
- If necessary administer first aid/ comfort to any injured persons and request ambulance.
- At this time secure the premises and do not touch anything in the area where the offence occurred. Place a notice in the front window stating you are closed due to an armed robbery.
- Isolate areas where the offender/s stood, touched, spat or bled immediately and indicate to police on arrival.
- Record all observations as quickly as you can after the robbery. Use the offender description form which is provided in this package.
- Please also note the offender/s level of aggression, tone, confidence or lack of, posturing, stance, weapons confidence, ordering and appearance. This may provide information as to the offender/s level of experience.
- Ask all witnesses to stay until the police arrive. Ask witnesses not to discuss the incident prior to talking to police. If a witness wants to leave, you have no right to hold them. Ask them to provide some identification and take down all their details. Provide this information to police as soon as they arrive. Offenders sometimes have accomplices posing as customers during a robbery.

How to assist the Police

Key things to remember:

- The time of the offence.
- The time the offender left the premises.
- The weapon/s used or implied.
- A description of the offender.
- What the offender took.
- Any evidence at the scene.
- The direction the offender left in.
- Any transportation of the offender used including type, make, model, colour, registration and number of occupants.
- Witnesses to the event (they should still be in the premises).

Victims

Victims of armed robbery frequently suffer trauma after the event. The police have victim liaison officers who can provide advice and assist you in accessing counselling.

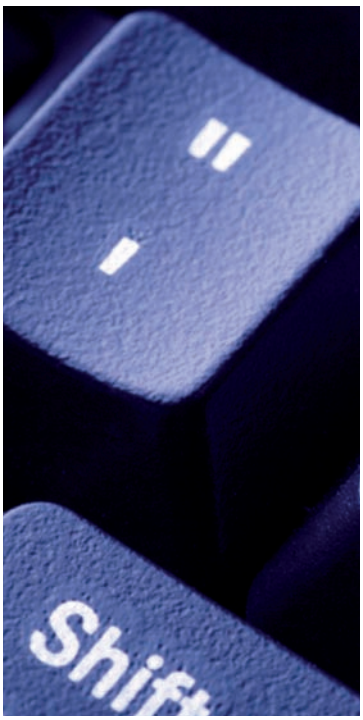
Victims of crime (Police assistance – ACT only)

Victim Liaison Officer
City Police Station
London Circuit, Canberra City
Telephone: 6245 7441
Email: Victims-Liaison-office@afp.gov.au

Internet Fraud

The term 'internet fraud' refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Internet fraud may include spam, scams, spyware, identity theft, phishing or internet banking fraud.



Spam

Spam is a generic term used to describe electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.

More information about spam is available from the Australian Communications and Media Authority (ACMA) website (**www.acma.gov.au**).

Scams

The power of the internet and email communication has made it all too easy for email scams to flourish. These schemes often arrive uninvited by email. Many are related to the well documented Nigerian Scam or Lotto Scams and use similar tactics in one form or another.

More information about scams is available from the Australian Competition and Consumer Commission (ACCC) SCAMwatch website (**www.scamwatch.gov.au**) and the Australian Securities and Investments Commission FIDO website (**www.fido.gov.au**).

Spyware

Spyware is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user. Spyware may take personal information, business information, bandwidth or processing capacity and secretly gives it to someone else. It is recognised as a growing problem.

More information about taking care of spyware is available from the Department of Broadband, Communication, and the Digital Economy (DBCDE) website (**http://www.Dbcde.gov.au**).

Identity theft

A large part of online crime is now centred on identity theft which is part of identity fraud and specifically refers to the theft and use of personal identifying information of an actual person, as opposed to the use of a fictitious identity. This can include the theft and use of identifying personal information of persons either living or dead.

More information about how to prevent and respond to identity theft is available from the Attorney-General's Department website (**www.ag.gov.au**).

Phishing

Phishing is a technique used to gain personal information for the purpose of identity theft. Phishing involves using a form of spam to fraudulently gain access to people's online banking details. As well as targeting online banking customers, phishing emails may target online auction sites or other online payment facilities. Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details. If the link is followed the victim downloads a program which captures his or her banking login details and sends them to a third party.

More information about phishing is available from the Australian High Tech Crime Centre (AHTCC) website (**www.ahtcc.gov.au**).

Internet banking fraud

Internet banking fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet banking fraud is a form of identity theft and is usually made possible through techniques such as phishing.

More information about internet banking fraud is available from the Australian High Tech Crime Centre (AHTCC) website (**www.ahtcc.gov.au**).

Suggestions to prevent loss from Online Fraud

- Consideration of using a low-limit separate credit card for online purchases to minimise the potential loss if things go wrong.
- Limiting the amount of personal information you allow to be 'the public domain' i.e.: social networking sites that could be used to assist in identity theft.
- Keeping anti-virus and firewall software up to date.

Credit Card and Cheque Fraud

Adopting thorough checking procedures can help protect your business from fraudulent credit cards and cheques.

Please remember you are under no obligation to accept credit cards or cheques as a form of payment and have the right to ask for photo identification.

Be alert for customers who:

- Buy an item with a cheque or credit card then return later to purchase more items. In some cases the initial purchase may be a chance to test out your policies.
- Travel from interstate to purchase items that are commonly available in their local city or town. They may be forced to shop outside their local community as they are known for using bad cheques or may be part of an organised syndicate travelling interstate to use fraudulent credit cards.

How to reduce credit card fraud

To help reduce credit card fraud against you and your customers, you can do the following:

- Do not enter the card details into the EFTPOS terminal manually without prior approval from the card issuer. Thieves using stolen credit cards will often damage the magnetic strip to avoid the card being identified by EFTPOS systems as stolen.
- Check card signatures.
- Check that the card numbers on the front and back of the card match.
- Make sure holograms are clearly visible, appear three dimensional and move when the card is tilted.
- Check the card is current by checking the "valid to" date.
- Check for ghosting or shading used to cover-up changed numbers.
- Ensure the transaction successfully processes before providing the goods to the customer.
- Ask for further explanation if unsure.
- It is preferable to sight the credit card being used but if accepting credit card payments over the telephone or internet request the customer quote the 3 or 4 digit security number printed on the back of the card and seek approval via the telephone from the card issuer.

- If taking telephone or internet purchases request a landline number in preference to a mobile number.
- Ensure credit card slips are disposed of in locked waste bins or shredded prior to disposal to prevent criminals from obtaining customer credit card details.

If you have any doubts ask to see a form of photo identification and ensure the person presenting the card is the rightful cardholder.

If you suspect a fraudulent card is being used at your business request identification and ask the customer to wait while you make further enquiries then contact police on 131444.

EFTPOS terminal security

Safeguard EFTPOS terminals by:

- Set an appropriate limit for refund or cash back for each EFTPOS terminal.
- Regularly change and keep confidential the EFTPOS password or PIN.
- Maintain physical security of EFTPOS terminals.
- Switch off your EFTPOS machine at night.

How to reduce cheque fraud

Accepting cheques as payment for goods or services exposes your business to the risks of accepting stolen cheques, counterfeit bank cheques, or cheques from accounts with insufficient funds to honour the cheque. To reduce the risks:

- Ask the customer for identification and make sure the identification offered is current and matches their physical description. Check the signature on the cheque matches the signature on the identification.
- Ensure the customer signs the cheque in your presence.
- Do not accept cheques that have been drawn in a bank interstate, even if the cheque is imprinted with a local address for the account holder.
- Ask the customer for their residential address if the only address provided on the cheque is a post office box number or another non-specific address. Ask the customer if the address on the cheque is their current address and ask for their phone number. Write these details on the back of the cheque along with the initial of the employee accepting the cheque.
- Do not accept post-dated or pre-dated cheques.
- Check there are no changes on the cheque.
- Check the figures match the amount in writing.

Bag Checking and Searching

There is currently no specific legislation dealing with a business owner's right to check a customer's bags or search a person. You can set conditions of entry ie. including presenting bags, parcels, cartons, or containers for checking by staff.

One method of displaying conditions of entry is using prominently displayed notices that clearly set out conditions of entry. The notices should be as large as practicable and displayed at a point where they can be seen clearly prior to entry to the business.

However, even though a customer may read the sign and enter the store he/she is under no legal obligation to allow a search of their bags, even a visual search. The business may ask to see inside the bag, but if refused they cannot demand.

Consensual bag checks

- Obtain verbal consent.
- Any request to check bags should be polite and courteous.
- Any checks conducted should minimise the degree of intrusion.
- Staff should request that the customer personally open the bag.
- Staff should not physically touch the customer or bag at any time.
- If an object obstructs the view into the bag, staff may ask the customer to remove the obstruction. Staff should not touch the obstruction themselves.
- If something is found inside the bag notify police and security immediately.

No consent for bag check

- Request that the customer speaks to the manager about the conditions of entry.
- Explain the conditions and point out the signs outlining the conditions of entry.
- Once you have explained the conditions, ask again to check the bag.
- Do not enter into arguments over checking any bags or suspected theft.
- Ask the person to leave.

You cannot arrest someone just because they have refused to let you check their bags. Unless you have reasonable grounds to believe an offence has been committed the customer is free to leave the store.

Training your staff

Anyone involved in checking bags should be trained properly in the legal procedures and requirements relating to bag checking. This should include citizen's arrest, shop stealing prevention and shop stealing detection.

Refusing entry of customer bags

There is no legal power to make customers place their personal bags in an allocated area. As such should an individual be requested or required to place their bag in a nominated area you may potentially be held liable for any losses received by the customers.

A person who attempts to enter the store carrying a bag may be refused entry.

Counterfeit Currency

Despite plastic banknotes being difficult to counterfeit there have been counterfeit notes circulated in the ACT. The majority have been $50 notes identified through incorrect feel, appearance and colour.

There are a number of security features on Australian banknotes which can help you to identify counterfeit currency, including:

- Printed on special polymer (plastic) – non genuine notes are often printed on paper and can be easily torn
- Raised print for the portrait and other major design elements
- Clear window with printed images or patterns which have clarity and are part of the bank note, not an addition
- Australian Coat of Arms which is visible only when you hold the note up to light

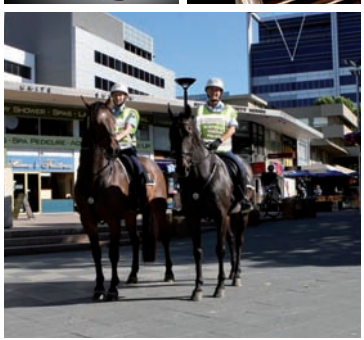
For more details about the polymer banknote security features, please read identifying counterfeit currency on the AFP website (**www.afp.gov.au**).

Ensure staff pay particular attention when banknotes are tendered for payment.

If you are given a banknote you suspect is counterfeit try to handle it as little as possible to preserve fingerprints, note the description of the person who tendered it and contact police on 131444.

ACT Keyholder Register

The ACT Keyholder Register is a list of the names and after hours contact details of business owners or others who have access to your business premises.



This information is stored on the AFP's confidential computer system and is not given out to anyone other than an authorised AFP staff member. The register is only accessed in the event police need to contact the business owner or another relevant contact person after hours.

Please make sure your current business details are on the register so police can contact the owner, or another nominated person to attend the premises in the event of damage from fire, burglary or other incidents that may happen after business hours.

You can update the register using our ACT KeyHolder Register online form, or use the ACT Keyholder Register PDF form available from the ACT Policing website (**www.afp.gov.au**). If you use the PDF form, please send it to the AFP address shown on the form.

Citizen's Power of Arrest

IS THERE A CITIZEN'S POWER OF ARREST?

In the ACT under section 218 (1) of the *Crimes Act 1900* for a person who is not a police officer to arrest a person **they must believe on reasonable grounds** that the other person **is** committing or has **just** committed an offence.

DO I HAVE A REASONABLE '**BELIEF**' THAT AN OFFENCE **IS BEING** COMMITTED OR **HAS BEEN** COMMITTED BY THE PERSON?
SUSPICION IS NOT ENOUGH

Belief on reasonable grounds

A state of mind where a reasonable person would also believe or accept as true that an individual is committing or has committed an offence.

For example: If you saw a customer take an item from the shelf, put it in their pocket and run out you have a belief on reasonable grounds.

Suspicion

Is where there is little evidence or proof that an individual is committing or has committed an offence, including where there is some uncertainty and doubt.

For example: theft buzzer sounds as someone exits the store; or a person has spent an inordinate amount of time browsing and is consciously avoiding assistance.

What can I do if I have a reasonable belief that an offence is being committed or has been committed?

Then you have grounds to arrest the person. If you fear for your safety it is recommended to let the person go particularly if the offender is known to you.

YOU MUST:

- Inform the person why they have been arrested, unless the suspect's actions make it impractical to do so.
- Contact Police immediately after arrest to transfer custody of person and property. It may be necessary to hold the person in a detention room for this to occur.
- Use only such force that is reasonable and necessary to affect an arrest. Excess force is not authorised and may constitute an assault.
- Ensure suspect is under constant supervision.
- Not remain in a secluded area with a suspect of the opposite sex.

YOU SHOULD:

- Identify yourself and your position and show identification.
- Ask the person to provide their name and address. However, they are under no obligation to answer any of your questions.
- Record statements made by the person and provided them to the Police.
- Take notes of events which can be later turned into statements for Police.
- Be mindful at all times of compromising evidence for the Police investigation.
- Ensure a citizen's arrest is conducted by a senior member of staff in the presence of a witness.

YOU MUST NOT:

- Conduct a search.
- Obtain a confession statement from the offender.

What can I do if I have a suspicion that an offence is being committed or has been committed?

You may approach the person and request to view contents of bag or ask them questions. If they refuse or offer no further evidence you have no power of arrest.

In this case you have no right to arrest a person, but if you suspect a crime has been committed you should contact the Police.

PLEASE NOTE:

Citizen's power of arrest is found in section 218 *Crimes Act 1900* (ACT).

Notwithstanding a lawful basis to arrest in some cases, attempting to intervene in such circumstances can be highly risky and in most cases it might be more appropriate to call police to attend.

Preventing Burglary

If your business becomes a victim of burglary the following may assist:

- Contact Police immediately on 000 or 131444.
- Do not touch anywhere the offender may have been and await instruction from the attending police. Try to protect any potential evidence from the weather.
- It is important that you have your street and shop number displayed at the front of your residence so that it is visible from the street to ensure that emergency services and visitors are able to locate your property easily.
- If you arrive at your business premises before police and you suspect the burglars are still inside, do not enter the premises, and wait for police to arrive.
- If the offender/s have left the scene and you are waiting for police to arrive begin compiling a list of what you think is missing. Include brand names, model numbers, serial numbers, accurate descriptions and any engraving details.
- Please ensure that you have provided current details for our ACT Keyholder Register (please refer to ACT Keyholder Register information sheet for details)

The following are some security measures you can implement to protect your business from burglary:

Warnings

- Warning signs may act as a deterrent, including signs stating: 'trespassers will be prosecuted' and 'no large amounts of money kept on premises'.

Keys

- Never leave spare keys hidden outside your business premises. Have a duplicate set of keys in a safe place, with someone you trust or in a secure location at home.
- Don't have personal details such as your name, address and telephone number on your keys.
- If you lose your keys or move into new premises, make sure you change all the locks.
- If someone calls you to say they have found your keys, tell them to drop them off at the nearest police station.
- Do not leave keys on the counter or any other obvious place.

Landscaping

- Landscaping should be maintained regularly with trees and shrubs trimmed away from doors and windows. This limits concealment and increases natural surveillance of your property.
- Obstacles and rubbish should be removed from property boundaries, footpaths, driveways, car parks or buildings.

Fences and gates

- If applicable, the boundary of the property should be clearly defined by boundary fences, preferably of open style construction. This allows greater visibility to and from the street, restricts unauthorised access and clearly defines your territorial space.
- Gates should be secured with quality hardened or alloy chains and padlocks.

Lighting

- External night lighting will enable police, security guards or passing people to monitor activities around the premises. The lighting should be directed towards the building as observers are likely to be outside the building.
- A limited amount of internal lighting should also be left on at night.

Power and switchboards

- Restrict unauthorised access and tampering with the power supply by housing the switch board within a metal cabinet and durable lock.

Doors, windows and glass

- Most burglaries occur at the side or rear of the buildings.
- Ensure door, windows and frames to the premises are secure and of solid construction.
- Ensure that doors and windows are correctly fitted and working property and that doors have quality deadlocks and that windows are fitted with key operated locks. Do ensure that this security does not trap occupants in an emergency.
- Glass within doors and windows can be reinforced by:
  1. reinforcing the existing glass with a shatter resistant film;
  2. replacing the existing glass with laminated glass; or
  3. installing quality metal security grilles or shutters.

Property marking

- Record descriptions, models and serial numbers of your business' property and keep this record in a safe place on and off site. **Serial numbers are essential in identifying property.**
- Property should be marked (engraved) with a number such as your ABN.
- Property which can not be marked should be photographed.

Safes and Tills

- Safes provide additional security for money, documents and other valuables.
- Safes must comply with Australian standards.
- Anchor the safe/till to the floor/ counter to prevent easy removal.
- Consider a time delay style safe incorporating a drop-chute to enable staff to deposit money without having to access the safe.
- Never keep large amounts of cash on the premises, particularly overnight.
- Leave your till empty with the draw open.

Alarm systems

- To enhance the physical security of your premises install a monitored intruder alarm system.
- Alarm system controls should be concealed to restrict tampering.
- Remote on/off switches should be strategically located.
- Movement detection devices should be strategically located around the premises.

Surveillance Equipment

- Cameras should be strategically installed inside and/or outside the premises to monitor areas of concern. Overt CCTV is likely to deter some crimes.
- When placing the cameras consider the potential for breakage, manipulation, spraying or smearing of the lenses with paint or grease etc.
- Cameras should monitor the cashier area and high cost merchandise or areas with poor supervision.
- TV monitors should enable staff to monitor activities on the camera.
- Recording equipment should be secured in a locked metal cabinet away from the main console area to restrict tampering or theft of equipment.
- Ensure video footage is of good quality by replacing tapes regularly. The ability to clearly identify and record faces, shapes and colours is essential in identifying offenders.

Fraud – Internal and External

Internal Fraud – Fraud by employees

Internal fraud includes employees undertaking any of the following actions:

- Theft of cash or stock.
- Theft from other employees.
- Not charging friends, family or accomplices.
- Allowing accomplices to use bad credit.
- Supplying receipts for refunds.
- Allowing friends to steal, or
- Participating in delivery scams.

Sometimes employees will rationalise the fraud by:

- Trivialising the offence: "They can afford it", "No harm done", "Everyone does it".
- Claiming unfair treatment as a justification.
  - Missing out on promotion.
  - Feeling remuneration is inadequate.
  - Unfair treatment compared to colleagues.
  - Disciplinary action.
  - Resentment at lack of appreciation.

The risk of internal fraud includes:

- Stolen, embezzled or 'discounted' stock.
- Loss of cash or securities.
- Loss of company funds or critical information, and/or
- Loss or damaged business reputation and custom.

You may be at risk of internal fraud by employees who:

- Work long hours.
- Return to work after hours.
- Are unusually or overly inquisitive about the company's payment system.
- Resist taking annual or sick leave.
- Avoid having others assist or relieve them.
- Resign or leave suddenly.
- Have a large number of voids.
- Have a low number of transactions.

How to reduce the risk of internal fraud:

Step 1: Develop clear policies that cover:

- Serving or processing transactions for family and friends.
- Personal purchases/transactions.
- Personal use of equipment such as telephones, lap-top computers, video cameras etc.
- Authorised delegations.

Step 2: Have clear transaction procedures, including:

- A pre-determined 'float'.
- Petty cash limits.
- Daily banking – by two people if possible.
- Dual signatures on cheques.
- Provision of receipts and acknowledgment of transactions.
- Limited access to safe by staff.
- Keeping registers closed unless in use, and
- Segregating purchasing, receipting and paying.

Step 3: Provide strong, consistent supervision of staff:

- Have supervisors monitor delegations.
- Supervise employee compliance with procedures.
- Regularly review cash shortages and report instances where an explanation is unsatisfactory.
- Have supervisors check receipts and documentation.
- Challenge suspicious transactions.

Step 4: Regularly review and monitor your register of assets and your transactions:

- Record all transactions.
- Conduct regular stocktakes.
- Keep a register of your tools, equipment and assets.
- Wherever possible, engrave your business property with an identifying number (such as your ABN).

Step 5: Establish strong audit procedures:

- Reconcile bank deposits with register totals regularly.
- Acquit all claims and allowances to avoid duplicate or multiple payments.
- Audit IT systems regularly.
- Conduct regular and random audits of all processes.
- Randomly check wages and allowances for overpayments.

Step 6: Maintain security of information:

- Limit access to confidential information.
- Enforce the use of employee ID.
- Regularly change passwords for computers, alarms etc.
- Review and investigate security violations.
- Cancel access promptly when people transfer or leave.

Step 7: Establish strong human resource management procedures:

- Undertake pre-employment screening.
- Implement equitable remuneration system.
- Provide job descriptions that segregate duties.
- Provide adequate training and education.
- Communicate policies, expectation of compliance, audit regime and consequences of non-compliance.

External Fraud – Fraud by customers

Please refer to the information sheet on credit card and cheque fraud.

External Fraud – Fraud by suppliers

External fraud by suppliers includes:

- Short or inferior supply of goods.
- Payment for services and goods not supplied.
- Kickbacks for biased selection of suppliers.
- Payments to bogus vendors for false claims.
- Cheques written for cash only or not property authorised.
- Purchase of goods for private use.

Fraud by suppliers can be prevented by:

- Ensuring staff are appropriately trained in accounts payable and stores functions.
- Ensure that supervision occurs over processing receipts and payments for expenditure.
- Ensure that purchasing, receipting and payment functions are segregated so that no single person performs all three duties.
- Ensuring there are guidelines for relationships between your business members and suppliers to avoid bias and inducements from suppliers (gifts).
- Ensuring audits are conducted on all areas of purchasing including petty cash, non-receipted items and all invoices.

Shoplifting Prevention and Detection

As most shoplifting offences are opportunistic crimes, the following steps can be taken to reduce theft:

- Acknowledge all of your customers and if possible keep customers in view at all times.
- Adequately light all selling areas.
- Always face your customers, especially when using the telephone.
- Always put merchandise away promptly.
- Always ensure keys are carried on the person or in a secure area and are not left on a counter or desk.
- Arrange store layouts for ease of supervising customers and stock.
- Count the day's takings in the privacy of an office and behind a locked door.
- Empty the cash drawer regularly to ensure the minimum amount of cash is present at any time.
- Ensure that price tickets are fixed securely to merchandise.
- Have a rapid and unobtrusive system to alert supervisors if there is any suspicious activity.
- Implement procedures to count the number of items being taken in and out of change rooms.
- Keep cash drawer closed at all times and do not leave it unattended.
- Move attractive and expensive merchandise away from exits or shop corners, etc. Place them in the middle of the merchandise area, raised areas or near the point of sale.
- Place the cash drawer in a position that cannot be reached by customers.
- Serve children as quickly as possible.
- Spend the maximum amount of time on the shop floor assisting customers, as opposed to being behind the counter.
- Never leave the shop front unattended.
- Try and ensure more than one staff member is working at a time.
- Use one way entrance and one way exit flow systems in self service units.
- Watch merchandise near the edges of the tables or counters.
- Watch out for customers who don't appear to be interested in purchasing items.
- Watch out for diversions.
- Watch out for overcrowding in general areas.
- Ensure that all employees are familiar with stock on display.

Detection

As a shop owner or employee, always be aware of customer diversions and within reason, remain suspicious. To assist in the detection of shoplifters, all business owners and employees should take note of the following:

- Customers carrying merchandise around the shop with them. You can advise the customer that you can hold the items at the counter whilst they look around.
- Customers carrying large or concealing items i.e. newspapers and large bags.
- Customer dress. Take note of customers who wear jackets, overcoats etc. when weather conditions do not require such attire.
- Customers who appear nervous, agitated or are acting suspiciously. You can approach the customer to ask them if they require assistance and/or reposition stock in their immediate area.
- Customers who leave your store very quickly.
- Customers who place bags on the floor while looking at stock. Items can be easily dropped into a bag before the business owner/employee has a chance to notice.
- Customers who refuse to be waited on.
- Customers who remain in the store for lengthy periods of time.
- Customers who frequently return to a particular spot within the store.
- Customers who refuse to look you directly in the eye.
- Customers who stand around rest rooms, stockrooms or stairways.
- Be aware of persons who pose as tradesmen, particularly those in unauthorised areas.
- Be aware of unsupervised school children in the store during school hours.
- Be aware of groups of two or more customers. One customer may be conspiring to distract your attention while the other customer steals the items.
- Tricks that customers may try to pull include:
  - A couple fighting in the store whilst a third person steals the goods.
  - Customers purposely falling over.
  - Customers dropping money or merchandise.
  - Customers spilling the contents of their purse, and
  - Customers faking illness.

If you do identify an offender, please use the offender description form provided in this package.

Workplace Security

Personal security measures:

- Never leave your purse or wallet in plain view or in the pocket of a jacket hanging on a door.
- Never leave cash or valuables at the office.
- Keep the business premises secure when working alone or before/after normal business hours.
- When working late try to find another worker or a security guard to walk out with you.
- Do not allow strangers to follow you into a secure area. Thieves often gain entry to buildings by 'tailgating' a legitimate staff member. Security and staff should question people who are not wearing identification and establish if they have authority for being on the premises.
- If you are in the elevator with another person, stand near the control panel so you are close to phone/emergency buttons. If someone gets into the elevator that makes you feel uncomfortable, get off immediately and wait for another elevator.
- Report all suspicious and criminal activity to the proper authorities: police, office manager and building security. Have emergency numbers displayed prominently.
- Know your escape routes and emergency procedures.

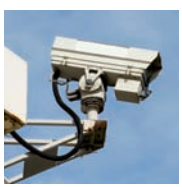
Business Premises security:

- Lock it up or lose it – Thieves usually look for items of value that can be easily sold such as laptop computers, mobile phones and cameras.
- Stay up to date – stay safe. Office security needs constant attention. A criminal offence against your business may be prevented by having up to date security measures in place and alert staff.

- Check security procedures for all building entry and exit points. Check for any faults and weaknesses in the security procedures you use. Thieves will take advantage of any opportunities to gain undetected access, such as through faulty fire doors and elevators, unattended loading docks and reception areas.
- Establish an assets register – Make sure your assets register contains the make, model and serial numbers of all your office equipment and is kept in a secure area.
- Nominate a security coordinator – It is recommended that one person in each office be nominated to be responsible for security issues. Their role should include: regularly conducting a security audit of the office, raising security concerns at staff meetings, liaising with other tenants or offices in the building, making recommendations to improve security and liaising with building security.
- Install security system warning signs to deter thieves – Warning signs at entry points to the building can inform a potential thief of your security system and deter them from entering the building.
- Network with other tenants about security issues – To have a broader understanding of the security issues that affect your office it is important that you liaise with building management and other tenants.
- Report all suspicious or criminal activity to Police – If you hear something or see something, say something.

Excluding Someone From Your Business Premises

Whilst the issuing of banning notices to customers is common practice among businesses, there are limited legislative options available to enforce this.



As a business owner or representative you may refuse entry to any person as long as the reason is not discriminatory e.g. if it is known that the person has been abusive to staff members, you can ask them to leave. This request revokes their lawful right to be there and they must be given the opportunity to leave. If the person returns to the store again the business owner or representative must again ask the person to leave and give them the opportunity to leave again. This can occur many times.

It is important that you attempt to identify the person and keep a record of their course of conduct. If the person's behaviour is disruptive or threatening call Police immediately and seek advice because they may be breaking the law. You will be provided with options for courses of action or it may be necessary for police to attend.

In situations like this police have a number of options which may be available to them including move on powers which is found in section 4 of the *Crime Prevention Powers Act 1998* (ACT). You may also be given advice on how to apply for a Workplace Order. The legislative provision for a Workplace Order is found in section 49 of the *Domestic Violence and Protection Orders Act 2008* (ACT).