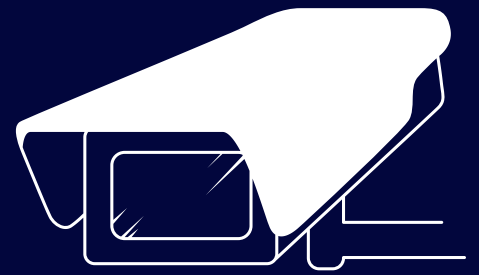
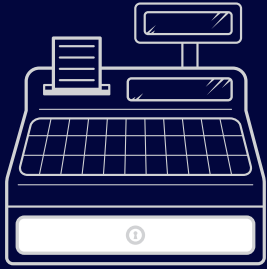




PROTECT YOUR BUSINESS



A MESSAGE FROM NSW POLICE FORCE



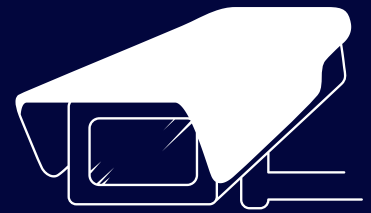
PROTECT YOUR BUSINESS

BUSINESS SECURITY	4
BUSINESS SECURITY CHECKLIST	5
SAFETY	6
ON THE STREET	7
IN YOUR CAR	7
RETAIL THEFT	8
LAYOUT & DESIGN	8
EDUCATE EMPLOYEES	9
CATCHING A SHOPLIFTER	10
AGGRESSIVE BEHAVIOUR	11
DEALING WITH CONFLICT	12
THREATS	13
PHONE THREAT CHECKLIST	14
EVACUATION	15
ARMED ROBBERY	16
PREVENTION	17
DURING AN ARMED ROBBERY	18
AFTER AN ARMED ROBBERY	19
OFFENDER DESCRIPTION FORM	20
CRIME SCENE	21
HANDLING CASH	22
EMPLOYEE THEFT	24
FRAUD	25
CREDIT CARD FRAUD	26
CARD NOT PRESENT TRANSACTIONS	27
MOBILE PAYMENTS	28
CYBERCRIME	29

This brochure will provide important security information for your business and allow you to carry out your own security assessment. If a major security upgrade is necessary for your business, it's advisable to contact a professional security company to carry out a security assessment.

Crime Prevention Command

BUSINESS SECURITY



Introducing simple crime prevention strategies into the way you conduct business can greatly impact the risk of becoming a victim of crime.

The main aim in increasing the security of your business is to increase the risk of the offender being caught or identified, to increase the effort it takes to commit the offence and to reduce the rewards received by carrying out the offence. The level of security your business should have is dependent on:

- The type of business or trade.
- The nature of the business or stock.
- The period of time that the premises are not occupied.
- The location of the premises.
- The history of offences on the premises / business.



BUSINESS SECURITY CHECKLIST

- Laneways and other external areas are well lit.
- Lighting is regularly inspected and is in working order.
- Trees and shrubs are pruned back to enable clear visibility between the street and the interior of the business.
- Boundary gates and fences are solid, well maintained and adequately secured with key locks.
- There is no rubbish or potential climbing aids near fences or around the perimeter of the building.
- All external doors and windows are secured with good quality locking devices. All doors should be of solid construction and properly installed.
- Steel door jamb are strengthened and fixed to frames.
- All padlocks are of appropriate standard.
- Concrete bollards, heavy planters or large rocks are placed in front of store windows to prevent ram raids.
- Monitoring alarm system is installed.
- Signs are displayed indicating the presence of a security system, the continual surveillance of your premises and any other security measures present.
- Electronic sensors are installed to advise employees when customers are entering and leaving your store.
- Maintain a key register and retrieve keys and access cards from employees leaving.
- Assess the need for installing surveillance camera/s or Closed-Circuit Television (CCTV).
- Posters and curtains on windows are minimised to ensure that visibility to and from the street is maintained.
- Safes are securely fixed to a solid object and are in close proximity to cash registers.
- All property of value is secured, and a register is maintained with details of make, model, serial number, description etc.
- All property is clearly and permanently marked with the name of your store, identifiable information or your Australian Business Number (ABN).
- All keys are accountable in a register and strict control of all keys are monitored. When not in use, keys are secured.
- Never leave large amounts of cash on premises overnight.
- Banking is conducted during working hours. Where this is not practical, ensure cash is placed in a secure safe and not taken home.
- All employees are aware and follow lock-up, emergency and evacuation procedures.
- Police and security are aware of emergency after hours contact information and key holders.
- Police are aware if you are a high risk commercial business or warehouse (i.e. store high value commodities such as cigarettes or electronic devices).

SAFETY

Under Work Health and Safety legislation, all people have the right to work in a safe environment in which risk to their health and safety is minimised. Employers have an obligation to provide a safe working environment. It is not always possible to be completely protected from harm, but we can take reasonable steps to reduce the risks.

SIMPLE TIPS THAT CAN MAKE YOUR BUSINESS A SAFER WORKPLACE

- Keeping doors and windows locked if you are working late.
 - Illuminating the store exterior at the front and rear of the store.
 - Providing adequate lighting at loading docks and the rear of the store, as these are usually hidden from general view.
 - Illuminating the store interior to an appropriate level. Well-lit stores will deter robbery.
 - Making sure there is adequate visibility from the street into your store.
 - Clearing the front window of excessive promotional material.
 - Advising someone when you are leaving.
- When designing the store layout, ensure clear visibility between aisles from the store counter and avoid leaving stock or rubbish on the floors during business hours.
 - Ensure all rear access points are safely locked and secure.
 - Surveillance camera/s or Closed Circuit Television (CCTV) may act as a deterrent and can greatly assist the Police in identifying offenders.
 - Pre-program important numbers such as 000 into your telephone and ensure all employees are familiar with emergency procedures and policies including how to deal with aggressive people, armed robberies, shoplifting and cash handling.

Other things you can do:

- Restrict access to employee areas.
- Secure the back rooms and employee only areas. Make sure that valuables such as personal possessions belonging to employees are locked away.
- Install audible door announcers to alert staff when customers enter the store.



SAFETY

SAFETY ON THE STREET

- When leaving, advise someone of your movements and expected time of return.
- Avoid walking alone at night unless absolutely necessary.
- Wear comfortable clothes that allow freedom of movement.
- Avoid taking shortcuts through dark, isolated areas.
- Walk purposefully and know where you are going.
- Walk on the footpath facing the oncoming traffic.
- If you feel threatened or followed, enter into a nearby business.
- Carry purses and handbags close to your body.
- Do not leave valuables such as mobile phones, handbags and wallets unattended, even for a moment.
- Carry a mobile telephone and personal alarm for security.

SAFETY IN YOUR CAR

- Park your car as close to work as possible. Have a friend or colleague walk with you on your return and have your car keys ready.
- When leaving your car, always remove the ignition keys, lock the doors and close windows.
- Check inside your car by looking through the windows before getting in.
- Drive with doors locked and the windows up.
- Do not leave valuable items visible inside the car.

RETAIL THEFT



Stealing is a common crime category often requiring a Police response. Reduce this crime occurring by implementing a few simple changes to your business.

STORE LAYOUT - SAFER BY DESIGN

- Store design should be open to allow good visibility across all areas.
- Stock and shelves should be neatly stacked and price tickets should be properly secured to goods.
- Elevate the cash register / counter area to improve employee view of the shop.
- Consider installing surveillance devices such as surveillance mirrors and Closed Circuit Television (CCTV).
- Use tickets / labels which cannot be easily removed.
- Where possible, lock expensive and easily portable goods in cabinets located close to staff working areas.
- Ensure that all selling areas are adequately lit.
- Warning signs regarding the consequences of theft and the security measures in place at your store, should be clearly displayed.
- Limit the number of entry and exit points to your store.
- Ideally, cash registers should be located close to exit points of the store and should be protected to prevent easy removal of money by offenders.
- Make sure that customers have no direct access behind the counter.
- Make sure you have clearly defined public and private areas.
- Employees should have a clear line of sight along the rows of shelving / display racks. If blind spots occur, install convex mirrors or mirror tiles behind stock shelving or cameras.

EMPLOYEE EDUCATION

With any type of business, it's important to educate and train all employees to understand their role and responsibilities.

WHEN TRAINING AND EDUCATING, ENSURE YOUR EMPLOYEES UNDERSTAND

- The store policy on bag checks and stealing.
- Procedures to follow if they suspect someone has stolen property.
- The safety of your staff and other customers.

ENCOURAGE EMPLOYEES TO;

- Acknowledge all customers.
- Pay attention to customers who are nervous or who appear distracted around merchandise.
- Approach and question people (even tradespersons) that stand around restricted areas, rest rooms, stock rooms, stairways or behind a counter.
- Be aware of people wearing loose overcoats and bulky clothing, especially in hot weather.
- Be vigilant of persons wheeling prams, shopping trolleys, carrying boxes and bags and other items that may assist in concealing stolen goods.
- Familiarise themselves with stock that is on display.
- Always keep customers in view and never turn your back on them.
- Never leave your sales area or cash registers unattended.
- Avoid leaving loose price tickets / labels within reach of the public, they may be swapped for a lower price.
- Check the price if a customer tenders an article for purchase and the ticket / label is mutilated, attached incorrectly, altered or missing.
- Examine all packaging on products for signs of tampering as other products may be hidden inside.

KEEP A WATCHFUL EYE ON

- Customers who do not appear to have a deliberate purpose to purchase items.
- Customers who remain in the store for lengthy periods of time, or who are 'sampling' merchandise that does not fit with their character.
- Customers who appear nervous, are perspiring, appear agitated or won't look you directly in the eye.
- Organised distractions where there are one or more persons attempting to commit thefts whilst distracting employees.
- Unsupervised children who are in the store during school hours.

CATCHING A SHOPLIFTER

Retail employees have a lawful right to apprehend or 'arrest' persons they have observed / witnessed committing a theft in their store. It is important that a set of procedures are put in place and that staff adhere to these procedures to prevent possible legal ramifications in the event of an unlawful arrest.

An arrest can only be effected on a person found committing an offence. The apprehension of a thief should always be made by the employee who has witnessed the theft, in company with another employee. The only occasion when this does not apply is if another employee has observed the theft on a video camera and has then relayed (e.g. via phone) the information to another employee.

The employee who witnessed the offence **MUST** be sure that:

- They've seen the goods being taken.
- They know where the thief has placed or concealed the item/s.
- They've maintained sight of the thief at all time, as the thief may have discarded the stolen item/s.
- The stolen item/s are still in the possession of the suspect and haven't been paid for.
- The suspect has passed the last possible point of payment.

If there is any doubt – do not arrest – Either way, call the Police!

If the thief has left the store and there is no doubt a crime has been committed, you may approach the person. Just remember to **NEVER**:

- approach them alone.
- be left alone with them, always have a witness present.
- touch the person, it may be construed as intimidation or assault.
- search the person, they may have sharp objects.
- accuse the person directly or indirectly of stealing.

A good approach to stopping a suspect is to politely approach them while identifying yourself and where you're from, then say:

"I believe you have some merchandise that you may not have paid for. We would appreciate you coming back to the store with us to straighten it out."

Await Police arrival.



AGGRESSIVE BEHAVIOUR

Over recent years there has been a marked increase in the number of incidents of employees being insulted or abused by aggressive, drug affected or mentally ill people, or customers who are dissatisfied with the service provided.

When dealing with an aggressive person it should always be remembered that the aggressive behaviour is not always directed at the individual but is targeted towards your position or organisation.

Every situation is different and as such there are no set procedures in dealing with aggressive persons. However, following some of these basic guidelines may assist employees in responding to such situations.

Assess the situation and remain cool, calm and collected at all times. If you believe that your safety and the safety of other employees or customers is at risk, then the police should be contacted immediately on **000**.

Patience is often the best strategy and this can be achieved by listening to the person and by acknowledging their problem or situation. Listening can be useful to allow the person to 'let off steam'. You must try to reduce the tension and calm the person down.



DEALING WITH CONFLICT

- ✗ Do not react to the customer's bad behaviour in the same manner.
- ✗ Do not let your guard down. Unstable people can be unpredictable.
- ✗ Do not let other employees get involved, but they should monitor for possible escalation of the incident.
- ✗ Do not take insults personally and always ensure you do not stand too close to the aggressive person.
- ✗ Do not enter the person's physical space as this can escalate the situation.

- ✓ Try to use counter areas or display stands to create distance and obstacles between yourself and the aggressor.
- ✓ Try to move the person away from any items that could be used as a weapon.
- ✓ Try to stay respectful, even if they're not respectful to you.
- ✓ Try to explain what options are available and encourage them to try one of these.
- ✓ Try to sense any change in behaviour and remember that over time, anger may diminish.

If you cannot calm a person down and they continue to be offensive or obnoxious, politely ask the person to leave your store. If they refuse, contact the Police immediately.

Employees are entitled to protect themselves, but only a minimal amount of force should be used. The force used to protect oneself against unlawful violence must be reasonable and necessary for such defence.

Excessive force is not justified and can result in a counter claim of assault.

In all instances of dealing with aggressive people, the main priority is to ensure the safety of yourself, your employees and your customers.

THREATS

Although rare, telephone and bomb threats are an issue that all employees should be made aware of. The procedures to be followed should be clearly explained to all employees.

TELEPHONE THREATS

Employees should be instructed that if they receive a threat, they should:

- Stay calm.
- Not panic or make return threats.
- Fill out as much information as possible on the: **'Phone Threat Checklist'**

Listen carefully and try to decipher:

- Sex of the caller.
- Age of the caller.
- Any accents or speech impediments.
- Any background noises.

Ask the caller:

- When the threat is to be carried out.
- Where the threat is located.
- What the threat is?
- Why?

DON'T HANG UP, keep the person talking to record more detail and keep the phone line open.



PHONE THREATS CHECKLIST

PHONE THREAT CHECKLIST	
KEEP CALM – Don't hang up! Keep the caller talking.	
TIME <input type="checkbox"/> am <input type="checkbox"/> pm	Did they identify themselves?
EXACT WORDING OF THREAT	
ASK What is it? (the threat)	
When will the threat occur?	
Where exactly is it?	
How will the bomb explode, or the substance be released?	
Did you put it there?	
Why did you put it there?	
Bomb Threat Questions	
What kind of bomb is it?	
What is in the bomb?	
What will make it explode?	
Chemical / Biological Threat Questions	
What kind of substance is it?	
How much is there?	
How will it be released?	
Is it a liquid, powder or gas?	
What will the substance do?	
Analysis of Caller	
SEX <input type="checkbox"/> male <input type="checkbox"/> female <input type="checkbox"/> unsure	ACCENT <input type="checkbox"/> Australian <input type="checkbox"/> British <input type="checkbox"/> American <input type="checkbox"/> Middle Eastern <input type="checkbox"/> Asian <input type="checkbox"/> European <input type="checkbox"/> Other type of accent? (specify)
VOICE Age estimate: _____ <input type="checkbox"/> angry <input type="checkbox"/> calm <input type="checkbox"/> loud <input type="checkbox"/> laughing <input type="checkbox"/> slurred <input type="checkbox"/> abusive <input type="checkbox"/> polite <input type="checkbox"/> incoherent <input type="checkbox"/> pre-recorded <input type="checkbox"/> read out <input type="checkbox"/> irrational <input type="checkbox"/> abusive Notes: _____	
BACKGROUND NOISES <input type="checkbox"/> traffic <input type="checkbox"/> animals <input type="checkbox"/> voices <input type="checkbox"/> machinery <input type="checkbox"/> music <input type="checkbox"/> noises on the line Notes: _____	
DO NOT HANG UP! Keep the line open - After the Call	
Your Name	Your Contact Number
Number Called	Date & Time Call Ended

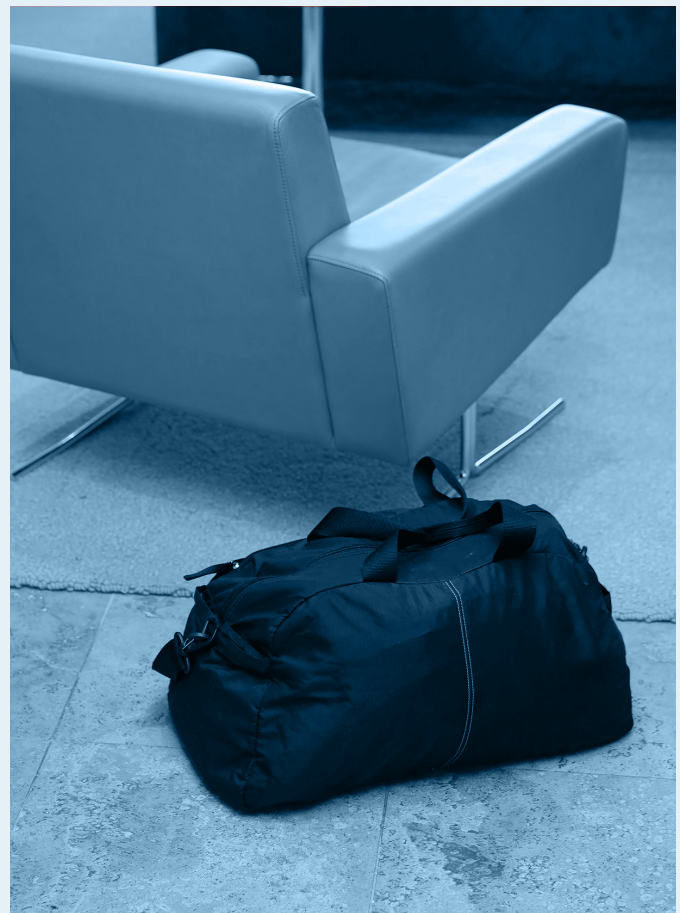
EVACUATION

If evacuation is deemed necessary, it should be conducted in a pre-planned and organised manner, similar to a fire alarm. Make certain all employees recognise the alarms and understand the procedures of evacuation. Ensure you have evacuation points chosen and clear instructions are in clear view for employees to see and follow.

LOCATING AN ITEM

If an item or suspect package is located:

- Do not touch, tilt or tamper with the item.
- Notify police immediately and follow the instructions given to you by them.
- Clear the area of all people.



ARMED ROBBERY

Criminals committing robbery offences are typically after cash.

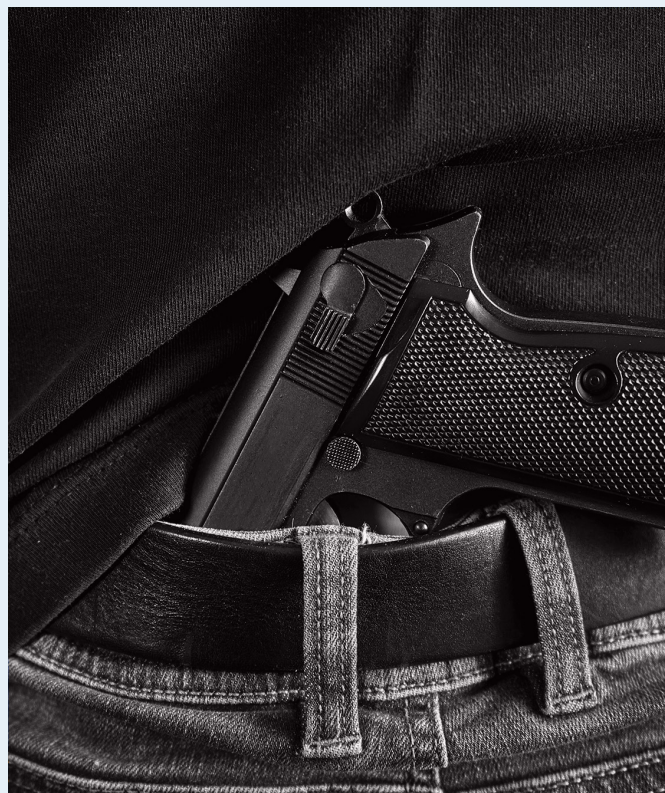
Businesses that deal in large amounts of cash and are open long hours, such as hotels, service stations and supermarkets are more commonly targeted, however any business can become the target of an armed robbery.

Whatever your business, it's important to have an Armed Robbery Plan in place. Do not wait until an Armed Robbery has occurred to implement an Armed Robbery Plan. With a small amount of planning, there are strategies and measures that can be taken to significantly reduce the risk of a robbery being committed and increase the chance of arresting the offender if it does.

The aim of an armed robbery plan is primarily to ensure:

- **Safety of employees and customers.**
- **Reduction in the property stolen.**
- **Fast arrest of the offender.**

Under the Work Health and Safety Regulation 2017 all businesses must have an emergency plan that provides for an effective response to an emergency and notifying emergency service organisations at the earliest opportunity. It is strongly recommended, emergency procedures incorporate a response to a robbery.



PREVENTION

- Be alert to strangers or individuals who are out of character or may be observing your business and are asking questions about how your business runs. It's a good idea to keep records of suspicious or odd activity, this information may be paramount to an investigation if a robbery occurs.
- Ensure doors and windows are kept locked and secure when not in use. If your business is open after normal business hours, consider having the main doors locked, with an intercom installed.
- Practice secure cash handling procedures
- Install safes with time delay locks and video surveillance.
- Make use of signage and stickers both inside and outside your business, promoting security measures such as: time delay locks, video surveillance and minimum cash held on premises.
- Consider the installation of a duress / panic button/s.
- Consider the use of find my device apps and placing tracking tags on high value items.
- Consider the installation of a security vestibule.
- Ensure areas where the Closed Circuit Television (CCTV) cameras are pointed, such as entries/exits and safe rooms are well lit. Install height markers on doors to judge offender/s height.
- Consider having a CCTV camera pointing at eye level to capture an offender's face if they are wearing a cap or hat.
- Avoid the opening and closing of the business by a single staff member.
- During opening and closing, limit staff movements in unsecured or exposed areas and ensure staff change their routine regularly and unexpectedly.
- Designate safe areas and escape routes for you and your employees.
- Ensure employees are aware of security and armed robbery procedures and what to do in the case of such an event. Have a priority list of who to contact.



DURING AN ARMED ROBBERY

The personal safety of staff and patrons is more important than any money or stock.

- Try to remain calm, assess the situation, and do exactly as the offender says. Remember that the number one priority is your safety, the safety of other employees and customers.
- Activate alarm devices as soon as possible, but only if it is safe to do so.
- Always remember that the offender will be nervous and tense, so explain any movements and avoid any sudden actions.
- Speak only when spoken to as any conversation with the offender will prolong the incident.
- Avoid eye contact with the offender.
- Note the offender/s conversation including any indecent language, accent, nicknames or speech impediments.
- Unless otherwise ordered, continually watch offender/s making a mental note of their description especially scars, tattoos and any other prominent features.
- Observe and take note of weapons that are being used.
- Observe the direction of travel taken by the offender/s when they leave the premises.
- Look to see if a vehicle has been used and if there are any other occupants.
- Never take drastic action during the robbery and do not chase the offender.
- **DO NOT** place yourself in danger to obtain additional information about offender(s) or vehicles.



AFTER AN ARMED ROBBERY

Your priority should be to ensure that first aid is administered to any injured or traumatised persons and to contact **000** even if you have activated hold up or duress alarms.

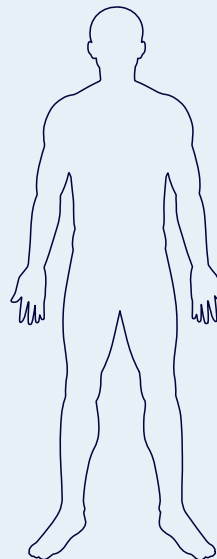
Upon calling **000** you will be asked for the following information:

- Name and exact location of where the crime occurred including closest intersecting street and business name.
- Date / time / nature of offence.
- Whether persons are injured and whether medical assistance is required.
- Type of weapon used.
- Number and description of offender/s including any vehicles used.
- Direction of travel when offender/s left the premises.



OFFENDER DESCRIPTION FORM

If you're a victim or witness to a crime, please complete this form by yourself. If you are unsure of an answer, don't guess - leave it blank. If there are other witnesses, record their names and ask them to record these descriptions on another form or piece of paper.



VICTIM / WITNESS DETAILS

Time/Date _____
 Name _____
 Phone _____
 Signature: _____

WEAPON

Knife Handgun Rifle/Shotgun Syringe
 Other Description: _____

VEHICLE DESCRIPTION

Registration	
Make	
Plate Colour/Style	
Model	
Type	
Colour	
Approx Age	
Other Features	

SEX male female unsure

Approx Age	
Height	
Weight	
Complexion	
Race	
Hair	
Facial Hair	
Eyes	
Glasses	
Headwear	
Upper Body	
Lower Body	
Shoes	
Bag	
Gloves	
Other (Jewellery, scars, tattoos, disguises, deformities etc)	
Behaviour (words spoken, accent, mannerisms etc)	

CRIME SCENE



- Only hang up the phone when told to do so and stay off the phone until police arrive unless you remember additional information that may be important.
- Close the premises to the public and keep unauthorised persons out.
- If possible, close the business to try and preserve the crime scene. If this is not possible, isolate areas the offender/s may have touched or walked.
- **DO NOT** clean the scene and try to preserve possible forensic evidence such as fingerprints and DNA, by not touching anything.
- Consider arranging someone to meet police outside, particularly in large shopping areas to make the response more efficient.
- Have witnesses and customers remain until the Police arrive. If you are unable to keep witnesses or customers there, obtain their names, addresses and telephone numbers for the Police.
- Make sure witnesses are isolated from each other to maintain independent recollection of events.
- Witnesses should independently try to write a full description of offender/s and what occurred in as much detail as possible. (Refer to the Offender Description Form)
- Do not make any statements to the media before discussing the matter with Police. Doing so could interfere with Police investigations or result in copy cat offences.
- Supply all details to police no matter how insignificant they maybe. This may also include earlier suspicious customers, rude, drunk or drug affected customers, cars constantly driving past etc.
- Investigators will require cooperation with a statement, any CCTV footage and possible follow up in criminal investigations or proceedings.

HANDLING CASH

The safe handling of your cash can assist in ensuring that you won't be a victim of crime. It is important that all employees with responsibilities for cash are aware of cash handling procedures. Cash handling incorporates not only general cash security, but also the secure storage and transportation of cash.

- Count cash in a safe and secure area of your store (out of public view) after you have checked the premises, (especially toilets, large cupboards etc) for persons who may have hidden themselves there.
- Have a telephone present in the room and consider installing a duress (panic button) alarm system or have a personal alarm system.
- Make sure that all exterior doors and windows are properly secured from the inside before counting money.
- Do not discuss cash amounts in public.
- Advertise that only a minimum amount of cash is kept on the premises.
- Use a safe that is securely fitted to a solid object.
- Do not take cash home.
- When leaving the premises at night, ensure your tills are left open and empty to protect against damage by thieves.
- Reduce cash held at counters to a workable minimum.
- Do not handle large amounts of cash or discuss cash holdings/movements in front of customers or in public.
- Vary the day and/or time of cash counts/ movements. Consider conducting cash counts during daylight hours rather than at close of business, particularly after dark.
- Do not transfer money between locations while wearing company uniforms. Vary the routine and route. If possible, utilise a contractor who specialises in cash transfers.
- Install a safe in close proximity to the cash register which is secured to a sturdy fixture or remove cash to a secure area.



HANDLING CASH

SET UP A SAFE WORKSPACE AND ROUTINE

- Not leaving the register drawers open longer than necessary.
- Position the cash register in such a way as to eliminate the public's view of its contents.
- Position the cash register so that it is out of reach of potential offenders.
- Keep as little cash in the register as possible, by regularly transferring it to a more secure place. Ensure this is done at random times.
- Do not keep large amounts of cash in your pockets while you are serving.
- Encourage employee vigilance. Watch for suspicious persons and vehicles and report observations, including descriptions, to the Police Assistance Line (**131 444**).
- Use EFTPOS for customer cash outs, to ensure that cash at the counter is kept to a minimum.
- All employees involved in cash handling should be regularly trained in correct cash handling procedures.

WHEN TRANSPORTING CASH TO THE BANK, VIGILANCE AND COMMON SENSE ARE NEEDED. CONSIDER THE FOLLOWING

- Where large amounts of money are to be moved, a cash transporting service should be utilised.
- Vary the route and the time you go to the bank –do not follow a pattern.
- Ideally, two employees who have been reference checked, are suitable and able-bodied, should be used in the transportation of cash to the bank.
- Company uniforms should not be worn or poorly covered. Badges should be removed from uniforms that would identify them as store employees.
- Do not place money or cheques etc into a handbag, bank bag or bag that identifies the store.
- Consider using an ordinary looking plastic shopping bag or a properly constructed cash carrying bag specifically designed to carry money.
- The money courier should walk facing oncoming traffic, away from the kerb.
- Be alert at all times to persons and / or vehicles following the money courier. Take note of registration and/or descriptions.
- If travelling in a vehicle, lock all windows and doors, ensure the vehicle is properly maintained and do not make any unnecessary stops on the way to the bank.

EMPLOYEE THEFT

It is unfortunate that theft by employees cannot be totally prevented, however, by implementing the following strategies, you can go some way to reducing this problem. Just remember that most employees are loyal to their employers and will work very hard and diligently on their behalf.

- All applications for employment should be carefully screened. References should be checked and any unexplained gaps in past employment should be explained. Ongoing and regular criminal history checks should be considered and police checks should be made on all new employees.
 - Provide strong and consistent supervision of all employees and immediately deal with issues of concern.
 - Ensure your policies are clear and explain what actions are not acceptable and liable to further action by management.
 - Adopt a 'prosecution policy' when dealing with employees. A successful prosecution in court should be widely publicised to act as a deterrent.
 - An induction program for new employees should be conducted providing them with a clear understanding of security procedures.
 - Provide ongoing retail security training programs to all employees.
 - Encourage employee contribution to retail security initiatives.
 - Arrange and clearly advise all employees as to the procedures to be followed in relation to employees purchasing goods from your retail outlet.
 - Put procedures in place that will make theft more difficult, which will also increase the possibility of getting caught.
- Have an effective asset inventory control system to identify losses as they occur.
 - All personal belongings should be locked away in a designated area.
 - Key control must be maintained at all times to ensure internal security.
 - Careful checks should be made at dispatch and delivery areas for the possibility of falsification of records, theft and signs of collusion between drivers and employees.
 - Ongoing issues in relation to short falls in daily takings should be investigated immediately.
 - Watch for customers and employees that continually use the same register together or regular customers that appear over friendly with employees.
 - Consider undertaking spot checks of bags if required.



FRAUD

HOW TO DETECT COUNTERFEIT CURRENCY

FEEL the note – a genuine note is printed on a special plastic polymer. It is difficult to tear and should return to shape if scrunched up.

LOOK at the note – a genuine note has multiple security features. There are different images printed on each denomination which makes each note unique.

Consider the use of Counterfeit Currency Detectors:

- Detectors emit a UV-light causing the security features of banknotes appear to shine.
- Detector units come in various designs that fit into the register and wall or desk mount.

If you think you have received a Counterfeit Note:

- Advise the person that you think that the note is counterfeit and that you are going to call the Police.
- Avoid returning the fake currency to the person.
- Handle the note as little as possible and place it in an envelope or other protective covering.
- Record the person's description and vehicle registration numbers (if sighted).
- Notify the Police straight away.

Polymer notes introduced in 1988



New notes introduced from 2016



For more information go to:
<https://banknotes.rba.gov.au/australias-banknotes/>

CREDIT CARD FRAUD

BE ALERT FOR A CUSTOMER THAT:

- Acts in an unusual manner.
- Is in a hurry, is nervous, blushes, talks hesitantly or is being overly chatty or friendly.
- Is making a purchase without regard to the price, quality or size.
- Who repeatedly returns to make additional charges.
- Wants to use PayWave more than once to avoid using a pin.
- Who brings the card straight out of a pocket instead of a wallet.

WHEN A CUSTOMER PRODUCES A CARD LOOK AT THE FRONT AND CHECK TO SEE IF:

- The card has a valid expiry date.
- The card is not damaged.
- That the embossing has not been altered.
- That the hologram does not appear to be suspicious.
- The card is not listed on the warning bulletin.

WHEN YOU CHECK THE SIGNATURE:

- Has the card been signed?
- Has the signature area been altered?
- Do the signatures match?

Ensure printed receipts match with the printed details on the card. Do not return the card to the purchaser before the sale has been processed and the signature confirmed. Always ensure you can view the card when the transaction is being undertaken. Should alterations or irregularities be found;

- **Ask for additional photo identification.**
- **Hold onto the card and call the Police on 000.**



CARD NOT PRESENT TRANSACTIONS

Internet, mail order and telephone credit card transactions are commonly referred to as 'Card Not Present' transactions. Businesses that accept Card Not Present transactions are at greater risk of becoming victims of fraud.

WHEN TAKING AN ORDER

- Obtain the credit card number, CCV number on rear of card, name of the bank, expiry date, full name, address and contact phone numbers.
- Confirm the order by calling the phone number provided to verify details.
- Make sure a reputable courier engaged by you makes the delivery.
- Only send deliveries to locations with a physical address. Never send to undefined places including parkland or enclosed areas.
- Ensure that the person making the delivery delivers the goods to a person inside the premises.
- Obtain a manual imprint of the card and signature wherever possible on delivery.



MOBILE PAYMENTS

Technology is advancing rapidly and mobile payments using phones, watches and other devices are becoming prevalent in business transactions.

HOW DOES IT WORK?

Users scan their credit/debit cards using an app. Common mobile payment apps use a security encryption method called tokenization to keep the card details secure on the device and during the transaction. Most apps will require multiple forms of identification from the device user during the transaction. Face recognition, iris scan, fingerprint and PIN numbers are the most common methods of identification.



MOBILE PAYMENT FRAUD

While most mobile payment frauds are committed through cybercrime, there are ways retailers can help reduce fraud committed during a customer transaction. Retailers should monitor customers behavior and look for irregularities. Particularly with customers having trouble authorising a payment and if purchasing exceeds the retailers predefined eftpos limits.

- Stay up to date with Australian industry standards.
- Buy and use only approved PIN entry devices at your point-of-sale.
- Buy and use only validated payment software at your point-of-sale or website shopping cart.
- Do not store any sensitive cardholder data in computers or on paper.
- Use a firewall on your network and PCs.
- Make sure your wireless router is password-protected and uses encryption.
- Use strong passwords. Be sure to change default passwords on hardware and software – most are unsafe.
- Regularly check PIN entry devices and PCs to make sure no one has installed rogue software or “skimming” devices.
- Teach your employees about security and protecting cardholder data.
- Follow the PCI Data Security Standard.

CYBERCRIME

Cybercrime and hackers are becoming much more prevalent as society and businesses move online. Hacking is when a scammer is gaining access to your personal information by using technology to break into your computer, mobile device or network. There are often warning signs that you have been or are trying to be hacked, such as:

- You are unable to log in to online accounts.
- Unusual icons on your display screen.
- Files have been deleted.
- You have an unexpectedly large internet/phone data or bill.
- There has been an unexpected charge to your bank account.

Here are some tips to help prevent you and your business from becoming a victim of cybercrime:

- Keep your personal information safe and secure.
- Secure your mail and letter boxes.
- Keep up-to-date antivirus software on devices.
- Have strong complex passwords for online accounts, particularly banking accounts.
- Keep WiFi and Bluetooth connections secure.
- Immediately report any lost debit/credit cards to your financial institutions.

- Report any thefts or crimes to relevant agencies.
- Always double check if a regular customer or supplier changes their payment information. It's a good idea to phone the customer or supplier and speak with them directly to confirm account payment changes.
- Maintain awareness of who you are communicating with. They may not be your customer. It is recommended you check the email address carefully; scammers will alter email addresses to look like those customers or suppliers you deal with.
- Commercially available software such as Adobe Professional can modify existing legitimate invoices.
- Be aware of emails with links to fake websites asking for users to update personal information and/or passwords.
- Be wary of callers needing remote access to your computer systems.
- Establishing procedures for invoice payments, such as limits of how much an employee can transfer without approval, can avoid significant losses.
- Always do your research if dealing with transactions using cryptocurrency.

Stay up to date with scams by going to

<https://www.scamwatch.gov.au>

CYBERCRIME

Business email compromise is when hackers gain access to a business's email system to scam organisations or customers out of money or goods. It's important to know:

- Criminals will edit legitimate invoices, using their own contact information or bank details to receive money or goods from organisations or customers.
- Criminals will impersonate an employee or organisation to change banking details with an organisation or customer to acquire money or goods.
- Criminals carefully research and monitor their potential victims or victim organisations. Criminals will register names, phone numbers and email addresses to closely match the victims.

If you have been the victim of business email compromise, follow the following steps as soon as possible:

- change any email or network passwords.
- notify anyone that may be affected, particularly your financial institution.
- report the scam to the NSW Police Force and the Australian Cyber Security Centre (ACSC).
- protect your stakeholders with a warning notice on your website or make personal contact with other potential victims.

For more information on Cybercrime business security visit <https://www.cyber.gov.au/>



REPORT THE CRIME 131 444

NSW POLICE ASSISTANCE LINE

If you have witnessed or become the victim of a crime immediately contact the NSW Police. Try and remember descriptive information on people, items or vehicles. When speaking to Police be helpful in answering all questions as accurately as possible and listen to instructions. There may be important evidence around so try to avoid touching the area as best you can until Police arrive.

NSW Police	<input type="text"/>
Street Address:	<input type="text"/>
City:	<input type="text"/>
Phone:	<input type="text"/>
Web site:	<input type="text"/>

It's always important to conduct your own or get a professional business security assessment. If you have any further questions, you can contact your Local Police Area Command or District and ask to get in touch with the local Crime Prevention Officer.

IMPORTANT NUMBERS:



Follow us on facebook.com/nswpoliceforce twitter.com/nswpolice youtube.com/thenswpolice or visit www.police.nsw.gov.au