

Best Practices For Preventing Ram Raids

International minimum security guidelines



Produced by the Global ATM Security Alliance

Table of Contents

Note to Readers	4
Introduction to Ram Raids	5-6
CHAPTER ONE - Physical Security for Stand-Alone ATMs Against Ram Raids	7-11
1.1 Securing the ATM Position	7
1.2 Anchoring the ATM	7
1.3 Recommended Further Security Measures	8-9
1.4 Additional Security Measures for Higher Risk Deployments	9-11
CHAPTER TWO - Physical Security for Thru-the-Wall ATMs Against Ram Raids	12-28
2.1 Definitions	12
2.2 General Recommendations - Risk Assessments	12
2.3 Comprehensive ATM Insurance as part of Risk Management	12
2.4 Minimum Recommendations	12-14
2.5 Site Preparation	15
2.6 Installation	15
2.7 ATM Anchorage	15-18
2.8 Installation in Wall	19-22
2.9 ATM Plinth	22
2.10 ATM Safe	22-23
2.11 Recommendations for Banknote Degradation Systems	23-24
2.12 Alarm Equipment	25-26
2.13 Control & Monitoring	26
2.14 ATM Activation	27
2.15 ATM Testing & Commissioning	27-28

CHAPTER THREE- Physical Security for Street-Based ATMs Against Ram Raids	29-33
3.1 Scope & Definitions	29
3.2 Risk Assessment	29
3.3 Installation	30
3.4 Recommended Security Measures	30-31
3.5 Recommended Additional Security Measures for Higher Risk Deployments	31-32
ADDENDUM "Recommended Lock Types"	33-34
Some Reported Successes	35-37
ACKNOWLEDGEMENTS	38
DISCLAIMER	38

Note to Readers

As a result of an upsurge in ram raids in several countries in 2005, an international Ram Raid think tank was convened by ATMIA.

The security guidelines listed are recommended as industry “best practice” and may be of assistance when putting together or reviewing an ATM security strategy for preventing ram raids. The document is a reference text and is intended to complement the advice of the Police, Insurers, Security Advisers, Security Departments of ATM deploying organisations and relevant National Security Standards currently in place.

It is recognised that different types of ATM installations – through-the-wall, stand-alone, telephone kiosk and column/pod - present different risks specific to the type of installation. Therefore, risk assessments remain the key to ATM security. Such assessments should take account of :

- the protection of the ATM and the structure in which it is contained;
- the safety of ATM users, the public, replenishers and service engineers;
- the cash rating of the security container fitted to the ATM ;
- the crime history of area;
- local police intelligence;
- the position or proposed position of the ATM.

Graham McKay, Executive Director, ATMIA Europe, recommends the following three components to an anti-ram raid strategy:

- Location of the ATM
- Physical security measures commensurate with risk assessment
- Banknote degradation system with a unique taggant deterrent

**Ram Raid Committee
Global ATM Security Alliance
June 2006**

Introduction to Ram Raids

Definition of Ram Raid

The Global ATM Security Alliance distinguishes between a ram raid and an ATM burglary. A ram raid is an attempt to remove an ATM, and its contents, from its location, usually after battering through to the ATM with a motor vehicle. An ATM burglary¹ is when an ATM is broken into, by a thief or an “insider”, to steal its cash.

A ram raid involves an attempt to rip the ATM out of its position and remove it from its premises with the intention of breaking into the machine later to steal its cash.

Ram raids often take place in the early hours of the morning in areas where police times might be slower than normal.

A variation of the ram raid is the rip-out. Here the premises or building are not ram-raided as such, but some form of construction plant with a bucket attachment is used to remove the ATM from the wall into which it is fitted.

Modus Operandi

A ram raid against **stand-alone, internally sited ATMs** typically happens like this.

The perpetrators use a motor vehicle to physically ram and breach the external perimeter of a premises or building and then steal from within it the complete ATM. The ATM could be lassoed, the lasso tied to a vehicle which then pulls away and removes the ATM from its anchoring. The cash is later removed from the ATM cassettes away from the premises.

There are numerous variations, but the three most common are:

- Vehicle used to ram-raid premises or building; chain, crane strap or similar is placed around ATM and then dragged out of premises using vehicle; once outside, the ATM is loaded onto the ramming or another vehicle.

¹ In the United Kingdom (UK) a ram raid of business premises is a criminal offence of burglary under Section 9 Theft Act 1968; the term ‘ram raid’ is shorthand for the method (modus operandi or MO) used to commit the burglary. GASA distinguishes the ram raid from a burglary by the fact that the ATM is first removed entirely from its position/location – this presents different security challenges from the ATM burglary committed on the premises.

- Vehicle used to ram-raid premises or building and then used to ram ATM with the intention of dislodging it from anchoring; once dislodged, the ATM is loaded onto the ramming or another vehicle.
- Vehicle used to ram-raid premises or building; suspect(s) then enter and physically uplift ATM and load onto the ramming or another vehicle.

Ram raids against **Through-the-Wall, externally sited ATMs** are often more sophisticated, as the external perimeter of the premises or building to be breached is usually more resistant to attack.

A typical MO would be:

- A more robust vehicle is used to ram-raid the premises or building such as a flatbed truck or large van, often with a piecing attachment strapped to it such as an RSJ; once the perimeter has been breached, the ATM will be dragged onto the vehicle using a winch or some other mechanical device.

The criminal operation is highly organised, often involving the use of 3 vehicles and industrial equipment. Usually, the ATM surround is chiselled out and an industrial wire is then placed around the machine. A large van is reversed towards the ATM, a wire is fed through the back and front (with the vehicle's windscreens removed) and attached to a tow bar on a second vehicle. The second vehicle pulls away and drags the ATM whole into the rear of the van.

A typical "rip-out" MO is:

- Construction plant is stolen from building site (often stolen immediately before the offence to reduce police intelligence) and then driven to the venue - the bucket attachment is used to breach the perimeter wall immediately surrounding the ATM and then used to scoop the ATM onto a waiting vehicle.

Ram Raids and Risk Assessments: General Recommendation

ATM deployments should always be preceded by risk assessments regarding the precise location of the ATM, which is critical to both business success, to ensure higher customer footfall to the site, and to ATM security. Risk assessments should include, where possible, consultation with local police as to the frequency of physical attacks on ATMs in the area. Locations may be classified as Low, Medium or High risk sites.

Chapter One

Physical Security for Stand-Alone ATMs Against Ram Raids

1.1 Securing the ATM Position

If the ATM is positioned in premises immediately adjoining to a road accessible to vehicles, it should be sited well away from perimeter glazing, particularly shop fronts, preferably directly against a strongly built internal or perimeter wall, which does not have vehicular access to its external face, and positioned to avoid a direct and unimpeded line of access from a door or other access point.

To reduce the risk of vandalism to the ATM and to increase user safety, the ATM should be positioned in a highly visible and well-lit area that allows maximum surveillance by counter staff and other customers.

Merchant-fill ATMs require 'line of sight' from the outside of the premises in order for the would-be offender to see clearly that the ATM has been de-cashed outside of business hours. The merchant fills the ATM prior to opening the premises and de-cashes after close of business, leaving the door to the ATM and security container open. An additional notice indicating that the ATM has been emptied of cash could be displayed in a prominent, visible place.

1.2 Anchoring the ATM

The ATM should be securely fixed to the floor through its security container by a minimum of four resin anchor bolts (minimum 12mm diameter to a minimum depth of 150mm) into a substantial concrete base.

Where a timber floor is involved the ATM should be bolted to a steel base plate by a minimum of four bolts, which is itself bolted through the floor joists by a minimum of four bolts.

When anchoring, reference should be made to the manufacturer's guidelines.

1.3 Recommended Further Security Measures

Once the ATM has been securely positioned on the premises and correctly anchored, it is important to decide on which additional security measures listed below will be required to counter the risks highlighted in the Risk Assessment. It is essential to implement the appropriate level of security as determined by the Risk Assessment.

1.3.1 Key security for CIT Fill ATMs

For CIT Fill ATMs, signs should be prominently displayed on the ATM and within the premises indicating that there are no keys available on the premises to allow access to the contents of the ATM.

1.3.2 Safe

The security provided by the security container (safe) within the ATM should be to a level commensurate with that required for the value of cash loaded in the ATM².

1.3.3 Intruder Alarm System

The premises should be protected by an intruder alarm system with monitored remote signalling to an Alarm Receiving Centre to a security level commensurate with the risk level:

- The system should qualify for the required local police response
- If it is a "confirmable" alarm system, a dual signalling facility should be provided
- The system should be designed to give the earliest possible warning of attack on the ATM
- Consideration should be given to including personal attack switches in the system

² Refer to the relevant BS/EN Performance Test Standards (EN 1143-1 & UL 291 standards)

1.3.4 Closed Circuit Television

Should the site Risk Assessment require it, the premises may be protected by a closed circuit television system, with or without detection facility, viewing the ATM, but **not** viewing the ATM keypad. It is the prerogative of ATM owners to decide which security technology and security strategies they wish to employ.

Its approaches should be linked to an Alarm Receiving Centre and recording equipment.

1.4 Additional Security Measures for Higher Risk Deployments

1.4.1 Definition of 'Higher Risk Deployments'

During initial site validation, or at subsequent site risk assessment visits, an ATM should be classified by the deployer as Low, Medium or High risk. Risk assessment criteria can depend on organisational, insurance and law enforcement recommendations and requirements. Industry advice may also be sought from industry approved consultants. It is recommended that details of site risk assessments be recorded in defined reports and stored in an organisational database.

1.4.2 External Measures

External approaches to the area of the premises where the ATM is sited should be protected by the installation of anti-ram bollards, vehicle-arresting systems, high rise kerbs, raised planters, reinforced lamp posts or similar street furniture, usually subject to local authority approval.

Where perimeter glazing extends down to the floor of the premises this should be protected by visually permeable metal roller shutters, security grilles or retractable anti-ram bollards configured to keep vehicles away from the vulnerable perimeter elements of the premises outside the premises operational hours.

1.4.3 Enhanced Anchorage

Instead of the anchoring system recommended in item 1.2 the ATM should be anchored by an enhanced anchoring system specifically designed to provide superior fixing for ATMs.

1.4.4 Security Collar or Anti-Lasso Device

A security collar, of the type associated with gaming machines, or an anti-lasso device, may be fitted where removal of the ATM is a risk.

Where such devices are deployed these should be attached to the main body of the ATM itself and not to the exterior facings.

1.4.5 Tracking System

The ATM may be fitted with a tracking system to enable its position to be determined in the event of theft of the ATM from the premises.

1.4.6 Banknote Degradation System

A banknote degradation system may be installed, which dyes/stains/degrades notes when activated in order to render them unattractive to thieves.

These systems are fitted to each ATM cassette, which holds notes contained in the ATM to provide a deterrent to theft of, or from, the ATM.

The banknote degradation system should be designed to activate immediately the ATM is moved or attacked by any means.

If required the system may incorporate a unique taggant, either 'bio technical' or 'chemical', although such identification systems should not be used in isolation.

Where a banknote degradation system is utilised notices to this effect should be displayed prominently around the perimeter of the premises and on the ATM itself. Banknote degradation systems may be linked to end-to-end solutions to maximise efficiency.

1.4.7 Security Fog System

A security fog system may be installed to protect the internal area of the premises where the ATM is installed to provide a deterrent to theft of, or from, the ATM.

These systems are designed to quickly block vision and disorientate in an enclosed area using a non-toxic substance to create the fog.

Such systems should be designed to activate immediately the ATM is moved or attacked by any means. The means of activation must be provided only when the area of the premises in which the ATM is sited is non-operational.

Where attack through the building roof is a possibility the security fog system should protect vulnerable roof voids.

Such systems must not negate any procedures associated with fire and emergency, particularly in means of escape in the case of an actual fire. It is recommended that advice be taken from the local fire safety officer before installation.

Where a security fog system is utilised, notices to this effect should be displayed prominently around the perimeter of the premises and on the ATM itself.

1.4.8 ATM Alarm System

In addition to alarming the premises consideration may be given to alarming the ATM itself.

This can be achieved by means of a stand-alone alarm system with its own unique reference number (URN).

The system should be monitored by remote signalling to an Alarm Receiving Centre and should qualify for an appropriate local police response.

If it is a "confirmable" alarm system a dual signalling facility should be provided.

The design should ensure that the system is armed at all times other than for maintenance for servicing and cash replenishment.

It should give the earliest possible warning of attack on the ATM.

In addition, consideration should be given to including personal attack switches for the use of CIT crews in the event of an attack during cash replenishment.

Chapter Two

Physical Security for Thru-the-Wall ATMs Against Ram Raids

2.1 Definitions

The primary focus of Chapter Two is on recommendations relating to the protection of “Thru-The-Wall” (TTW) ATMs against physical or brute force attacks. For the purposes of cash replenishment, the scope of this document is limited to the security of a TTW type of Automated Teller Machine (ATM) located at a Bank Branch or at self-service bank locations. Because of this the assumption is made that cash replenishment will be conducted by Bank Branch staff, not by an external service supplier. For TTW ATMs installed at other types of locations (hypermarkets, petrol stations etc) and requiring cash replenishment by a commercial security organisation, please refer to Chapter One.

A Thru-the-Wall ATM does not stand on its own but is installed within the wall of a building (interior or exterior) to which it is affixed to allow customers to conduct transactions at the ATM outside of, or even away from, a bank branch. This type of machine contrasts with Stand Alone ATMs, which are not fixed within the wall of a building.

2.2 General Recommendation – Risk Assessments

It is recommended that a risk assessment of each location be carried out as outlined in Chapter One. It is also recommended that each ATM deploying organisation conducts a detailed and thorough ATM risk analysis for their own country, and geographical areas of operation, and that based on this, a detailed ATM security strategy is prepared or up-dated.

2.3 Comprehensive ATM Insurance as part of Risk Management

ATM site owners/managers should proactively ensure that their insurance company is aware that an ATM is to be installed on the premises, checking exactly what cover is included in the existing policy and what reviews need to be made to it. All risk scenarios should be assessed, including the risk of a ram raid on the ATM, with all of its potential liabilities.

2.4 Minimum Recommendations

This section assumes that the deployer has carried out site validation and submitted a site validation report (see GASA’s [Best Practices for Physical ATM Security](#) Version 2), including a full risk assessment.

2.4.1 Installation Contractor Responsibilities

The Installation Contractor³ should be responsible overall for the transport, installation, anchoring of the ATM, and for the testing and commissioning of the software as follows:

A	Site Validation
B	Software testing and commissioning
C	Site Handover
D	Site Photographs
E	Checking that all security requirements are being adhered to
F	ATM Transportation
G	ATM Installation
H	ATM Anchoring

2.4.2 Base Composition

During the Site Validation an assessment should be made of the base to ensure that it is of sufficient strength and depth to anchor the ATM. It is recommended that screed is not included in any measurements of base depth.

2.4.2.1 On Solid Ground

➤ Use Existing Base

If it is deemed possible to use the existing base, the existing concrete should be reinforced and of a minimum depth to meet the requirements of the anchor bolt manufacturers.

The ATM can then be anchored directly into it (provided that the base height is not required to be raised – see section entitled “Base Height” below).

➤ Plan For New Base

If it is not possible to use the existing base without modification, then a plan should be made to strengthen the base.

When making this plan a minimum depth of 150-200mm reinforced concrete should be retained with the existing base, in order to anchor the new base to it.

³ The Installation contractor may be the ATM Supplier, or may be a third party working for either the ATM Deployer or the ATM Supplier

2.4.2.2 Above A Cellar/Basement

For anchoring to take place above a cellar or basement:

- Base Depth

It is important that the existing concrete floor is at least 150-200mm in depth.

2.4.3 Base Height

In order to anchor the ATM properly it is important that accurate measurements are taken during the Site Validation Visit. The use of 'pilot holes' may be required if the depth cannot be determined by other methods.

For the ATM to be properly anchored it should be able to sit on a plinth that will enable it to exactly reach the required height.

2.4.4 Report Distribution

It is recommended that the report be distributed to the following parties:

- ATM Deployer – Security Representative
- Installation Contractor
- Bank/Site Property Department
- Bank/Site Security Department
- Branch/Site Manager
- Building Contractor
- Security Contractor

2.5 Site Preparation

Any contract relating to the deployment of an ATM should clearly define the party (or parties) responsible for taking the following actions:

- The preparation of the site (including physical protection against “ram raids”)
- The provision, installation, testing and commissioning of all security equipment
- The provision of a dedicated telephone line (if required).
- The ATM Base preparation (as required)
- The electrical preparation (as required), including the provision of clean power.

2.6 Installation

Any contract relating to the deployment of an ATM should clearly define the party (or parties) responsible for taking the following actions:

- The installation, testing and commissioning of all security alarm equipment
- The installation, testing and commissioning of the Lock (testing and commissioning only if the lock is pre-installed by the ATM Supplier)
- Defining and ensuring compliance with all general Site Requirements (i.e. parking)
- The provision of all plans/documentation relating to the construction of the building

2.7 ATM Anchorage

Secure anchoring may be done under the following scenarios:

2.7.1 Anchoring Plinth To Base - No Cellar - Sufficient Concrete

This assumes that the ATM will be anchored into solid ground with sufficient concrete. Sufficient Concrete is reinforced concrete to a minimum depth required for the length of bolt used. For details of required depths it is recommended to consult the handbooks of the major anchor bolt manufacturers.

2.7.1.1 Anchoring Method - Installation Contractor

The installation contractor should anchor the ATM in accordance with the relevant CEN (or other) standard relating to the grade of safe used.

2.7.1.2 Anchoring Certificate - Installation Contractor

The Installation & Maintenance Contractor should complete a Certificate stating that the anchoring has been done in accordance with these requirements.

All exact measurements relating to the anchorage should be recorded.

A copy of this Certificate should be passed to the ATM deployer for audit purposes.

2.7.2 Anchoring Plinth To Base - No Cellar - Insufficient Concrete

This assumes that the ATM will be anchored into solid ground with insufficient concrete. Insufficient concrete is concrete that is not reinforced and does not meet the minimum requirements of the anchor bolt manufacturers. When this is the case a concrete base should be constructed and properly attached to the existing floor.

2.7.2.1 Base Preparation - Building Contractor

When preparing a base the Building Contractor should follow the minimum requirements of the anchor bolt manufacturers. Guidelines for the preparation of a 30cm base are as follows:

A	The base should be constructed using as standard two U-sections (UPN 160 - 160mm x 65mm x7.5mm). Larger U-sections may be used depending on the required height of the base.
B	Minimum of 16 x Steel (BE50) Rods (4x4) should be used to anchor the base to the floor. These Rods should be 12mm diameter.
C	They should be anchored into holes drilled to a depth of 8cm and with a diameter of 16mm. The anchoring should be done using Chemical Paste.
D	A Steel Grid (BE50 - 150mm x 150mm x 8mm x 8mm) must be constructed to lie on top of the Steel Rods.
E	The existing floor surface must be roughened and wetted.
F	Concrete (Class C40/50) must be poured into the construction, which must meet a crush resistance of 35N/mm ² after 7 days.

2.7.2.2 Base Construction Certificate - Building Contractor

The Building Contractor should provide a Certificate stating that the Base has been constructed and anchored in accordance with these requirements.

A copy of this Certificate should be passed to the ATM deployer for audit purposes.

2.7.2.3 Anchoring Method - Installation Contractor

The installation contractor should anchor the ATM in accordance with the relevant CEN (or other) standard relating to the grade of safe used.

2.7.2.4 Anchoring Certificate - Installation Contractor

The Installation Contractor should complete a Certificate stating that the anchoring has been done in accordance with these requirements.

All exact measurements relating to the anchorage should be recorded.

A copy of this Certificate should be passed to the ATM deployer for audit purposes.

2.7.3 Anchoring Plinth To Base Over A Cellar

This assumes that the ATM will be anchored over a cellar/basement/garage to which the public may or may not access, and for which entry/egress control may or may not be under the direct control of the Bank, or other Thru-the-Wall ATM deployer.

After the Site Validation visit, the ATM Deployer Security Representative should approve the proposed anchoring plan.

2.7.3.1 Anchoring Method - Installation Contractor

The installation contractor should anchor the ATM in accordance with the relevant CEN (or other) standard relating to the grade of safe used.

2.7.3.2 Anchoring Certificate - Installation Contractor

The Installation Contractor should complete a Certificate stating that the anchoring has been done in accordance with these recommendations. All exact measurements relating to the anchorage should be recorded.

A copy of this Certificate should be passed to the ATM Deployer for audit purposes.

2.8 Installation in Wall

2.8.1 Solid Wall

If accessible from an area with vehicular access, the ATM should always be installed behind a solid brick or concrete wall. If one does not exist, it should be constructed.

If this is not possible, the options laid down under “Steel Section Wall” and “Steel Girders (HEB-100 Sections) below should be followed, and should be approved by the ATM Deployer – Security Department.

2.8.1.1 Wall Construction - Building Contractor

The Building Contractor should construct a wall that must be at least 14cm thick and with a mass of 1,900 kg/m³. Any deviations from the above should be cleared with the ATM Deployer before installation takes place, and should be shown in the Construction Certificate.

2.8.1.2 Construction Certificate - Building Contractor

The Building Contractor should provide a Certificate stating that the wall does comply with the required standard and stating the exact composition and depth of the Wall.

A copy of this Certificate should be passed to the ATM Deployer for audit purposes.

2.8.2 Steel Section Wall

In the event that it is not possible to install the ATM behind a brick or concrete wall, then the next preferred method is to install it behind a solid steel section.

2.8.2.1 Steel Section Anchoring To Floor - Building Contractor

The Building Contractor should anchor the steel section to the floor as follows:

A	Use a minimum 4 x M10 Chemical Bolts
B	Anchoring only to be done in concrete - minimum depth 9 cm.
C	Manufacturers anchoring requirements should be mandatory
D	Non-destructive quality control of the anchoring should be made (resistance up to 25-35Nm)

2.8.2.2 Steel Section Anchoring To Ceiling/Walls - Building Contractor

The Building Contractor should anchor the steel section to the ceiling/walls as follows:

TO CONCRETE CEILING	
A	Minimum 4 x M10 chemical bolts
B	Anchoring only to be done in concrete - minimum depth 9cm.
C	Manufacturers anchoring requirements are mandatory
D	Non-destructive quality control of the anchoring has to be made (resistance up to 25-35Nm)
TO BEAMS	
A	The anchoring must be done directly into the Beam
B	If required a 'bridge' can be made using a Profile 60mm x 60mm x 4mm, to be anchored with 4 x M10 bolts
TO WALLS	
A	Anchoring must only be done in the mortar between the bricks with chemical bolts
B	There must be 2 x M10 Bolts every 50cm with a minimum depth of 9 cm. In the corners, top and bottom, a 15cm x 15cm steel plate must be used.
C	In cement blocks 1 x M10 bolt with injection of chemical paste must be used, with the anchoring at least 15cm from the edge of the block.

2.8.2.3 Construction Certificate - Building Contractor

The building contractor should complete a Certificate stating that the construction and anchoring has been done in accordance with these requirements.

All exact measurements relating to the construction and anchorage should be recorded.

A copy of this Certificate should be passed to the ATM Deployer for audit purposes.

2.8.3 Steel Girders (HEB-100 Sections)

In the event that it is not possible to install the ATM behind a brick or concrete wall, or a steel section, then the next preferred method is to install it behind steel girders.

2.8.3.1 HEB-100 Section Construction - Building Contractor

The Building Contractor should ensure that HEB-100 sections (or equivalent) are used for the frame as follows:

A	The HEB-100 sections should be installed on both sides of the ATM
B	The distance between the base sections must not exceed 1.25 Metres (and must be as small as possible)
C	If telescopic hollow sections are used, both sections must overlap for at least 50cm.
D	2 x Cross sections (hollow section casing profiles 80mm x 60mm x 6mm) must be attached to the H-Sections, above and below the outer edge (or 'nose') of the ATM.
E	Each Cross section must be a hollow section of 80mm x 60mm x 6mm.

2.8.3.2 HEB-100 Section Anchoring To Floor - Building Contractor

The Building Contractor should anchor the HEB-100 section to the floor as follows:

A	Use a minimum 2 x M10 Chemical Bolts
B	Anchoring only to be done in concrete - minimum depth 9 cm.
C	Manufacturers anchoring requirements should be mandatory
D	Non-destructive quality control of the anchoring should be made (resistance up to 25-35Nm)

2.8.3.3 HEB-100 Section Anchoring to Ceiling – Building Contractor

The Building Contractor should anchor the steel section to the ceiling as follows:

TO CONCRETE CEILING	
A	Minimum 4 x M10 chemical bolts
B	Anchoring only to be done in concrete - minimum depth 9cm.
C	Manufacturers anchoring requirements are mandatory
D	Non-destructive quality control of the anchoring has to be made (resistance up to 25-35Nm)
TO BEAMS	
A	The anchoring must be done directly into the Beam
B	If required a 'bridge' can be made using a profile 60mm x 60mm x 4mm, to be anchored with 4 x M10 bolts

2.8.4 Construction Certificate - Building Contractor

The building contractor should complete a Certificate stating that the anchoring has been done in accordance with these recommendations. All exact measurements relating to the anchorage should be recorded.

A copy of this Certificate should be passed to the ATM Deployer for audit purposes.

2.8.5 Anchoring Certificate - Installation Contractor

The Installation Contractor should complete a Certificate stating how the anchoring has been done. All exact measurements relating to the anchorage should be recorded.

A copy of this Certificate should be passed to the ATM Deployer for audit purposes.

2.9 ATM 'Plinth'

2.9.1 Plinth Type Required

When deciding on an ATM plinth, ATM deployers should assess its construction from a security perspective. Plinths specially constructed to withstand 'ram raids' and other brute force attacks may be considered for higher risk locations.

2.9.2 Anchoring ATM To Plinth

For installers using CEN approved plinths, the anchoring arrangements should be those that are approved in the CEN documentation for that product. The correct implementation of those arrangements will guarantee good anchoring.

2.10 ATM Safe

It is recommended that a strong ATM safe be used to protect cash inside the ATM. The grade of safe used can be varied depending on the area risk assessment as follows:

2.10.1 Safe Type Recommended – High/Medium Risk Area

For higher risk areas it is recommended that a minimum CEN 3⁴ (or equivalent) safe be used. This can be lowered to a UL 291 Level 1 safe used in conjunction with a banknote degradation system (either cassette based, or integral to the ATM).

⁴ Refer to EN 1143-1 for full grading and security capabilities of CEN safes.

2.10.2 Safe Type Recommended - Low Risk Area

For areas defined as lower risk it is recommended that a UL291 Level 1 safe be used. A banknote degradation system (either cassette based, or integral to the ATM) could be installed as an optional extra.

2.10.3 ATM Lock Recommendation

For CEN Safes and UL Safes appropriate high security locks are compulsory and will have been fitted to gain the required safe grading. To ensure that this is the case, the ATM must have a security label attached, showing the grading of the safe.

If the ATM does not have such a label, or if the safe is being upgraded with another lock after the ATM has been delivered, an EN 1300 Grade B or UL Group 2M lock or equivalent are recommended.

Please see Addendum "Recommended Lock Types".

2.10.3.1 ATM Lock Installation - Security Contractor

For installed ATMs where a Bank requires a Time Delay/Time Lock, the Bank's security contractor should fit it in accordance with the manufacturer's requirements. It should then be connected to an appropriate Central Monitoring Station (CMS) and a test made.

For ATMs supplied with locks which have external alarm monitoring capabilities, the lock should be connected to an appropriate CMS and a test made.

2.10.4 Control and Monitoring

If there is a requirement to monitor the status of a remotely monitored lock, it should be monitored from an appropriate CMS 24 hours daily. The CMS should automatically generate an alarm signal if the telephone line fails or is cut.

The CMS should be able to monitor the functionality required by the ATM deployer e.g. lock open/closed, time access windows.

2.11 Recommendations for Banknote Degradation Systems

An independent test house should check any banknote degradation system used, and should certify that it does operate according to the manufacturer's claims.

Such a system should meet any national standards relating to usage of banknote degradation systems.

Banknote degradation systems should also be tested on real banknotes and be verified that the degrading agent is safe, and that the required percentage of the notes are degraded on the required percentage of the printed area.

Some banknote degradation systems can link with CIT intelligent systems to provide end-to-end security between the ATM and the cash centre.

See also 1.4.6 of Chapter One.

2.12 Alarm Equipment

The following alarm equipment is recommended for installation at each ATM location:

Seismic Detector	A seismic detector should be fitted to the ATM safe door.
Magnetic Contact	A magnetic contact switch should be fitted to the door of the ATM Safe. A magnetic contact should also be fitted on the door of the ATM Technical Room. This should be on a different circuit to the alarms fitted to the ATM safe.
Volumetric Detector	A volumetric detector should be placed on the wall of the ATM Technical Room. This should be able to detect any movement in the area surrounding the ATM. This should be on a different circuit to the alarms fitted to the ATM safe. If the Bank Branch has a cellar, which is under its direct control, a volumetric detector should be fitted to cover the area underneath the ATM anchorage.
Personal Attack Switches	Personal Attack Switch(es) should be fitted in the ATM Technical Room as close as possible to the ATM. This is to provide protection to staff servicing or replenishing the ATM.
Alarm Control Panel(s)	An alarm control panel (key or combination) should be fitted at the technical room door. If this panel is able to control two circuits, then an additional panel does not need to be fitted in the vicinity of the ATM. An alarm control panel (combination) should be fitted in the immediate vicinity of the ATM.
Closed Circuit Television (CCTV) (Optional)	CCTV cameras may be installed covering the external face of the ATM (without the facility to view the ATM Pin Pad) and the rear of the machine in the technical room. Images from these cameras should be recorded and backed up as required.
Access Control	Where possible, access to the rear of the ATM should be restricted and a door swipe or keypad system should be used to control the technical room door.
Heat Sensor	A heat/smoke sensor should be fitted inside the ATM. This should detect any form of oxy acetylene or burning bar attack on the ATM, and should be on the ATM security circuit.

2.12.1 Alarm Equipment Installation - Security Contractor

All equipment should be correctly fitted in accordance with the manufacturer's specifications.

Once the equipment has been fitted a live test of each item mentioned above must be conducted and a check made that the Central Monitoring Station picked up each signal.

2.13 Control & Monitoring

2.13.1 Central Monitoring Station (CMS)

The alarm system should be monitored from a CMS 24 hours daily. The CMS, which should conform to ISO and local police standards, should automatically generate an alarm signal if the telephone line fails or is cut. In the event that an alarm signal is received, the CMS should respond according to its standard operating procedures.

2.13.2 Response

In the event of an alarm the CMS should be able to request a response from a third party to visit the ATM within an agreed (ideally contractually binding) time period.

2.13.3 System/Line Failure

In the event that the alarm detection system fails to operate for any reason, or there is a fault in the telephone line, the ATM should be cleared of all cash until such a time as the system is operational and has been tested.

2.14 ATM Activation – “online status” – Pre-Conditions

ATM Anchored and Protected Against Ram Raids	
A	A Construction Certificate should have been completed by the Building Contractor (if required) and passed to the ATM Deployer.
B	An Anchoring Certificate should have been completed by the Installation Contractor and passed to the ATM Deployer.
	<i>See Paragraphs on ATM Anchorage, ATM 2.8 Installation in Wall, and 2.9 ATM 'Plinth' for further information.</i>
ATM Security Equipment Fitted	
	The correct alarm equipment should have been fitted, connected to the Central Monitoring Station and tested.
	A suitable lock should have been fitted, able to meet all the current requirements.
	<i>See Paragraphs on 2.10.3 ATM Lock Recommendation and 2.12 Alarm Equipment for further information.</i>

2.15 ATM Testing & Commissioning

The following steps should be followed for an ATM to be tested and commissioned:

2.15.1 Authorisation

Prior to dispatching a Technician to the ATM site, the Installation Contractor⁵ should check with the ATM Deployer that all the Pre-Conditions (as outlined in the above table) have been met.

2.15.2 Field Test & Network Connection

On arrival at the ATM site the Installation Contractor's Technician should conduct a thorough test of the ATM and connect it to the ATM network.

2.15.3 Test Certificate

On completion the Technician should sign a Test Certificate to confirm that everything is correct and that the ATM is ready to go 'live'. A copy of this Certificate should subsequently be sent to the ATM Deployer.

⁵ The Installation contractor may be the ATM Supplier, or may be a third party working for either the ATM Deployer or the ATM Supplier

2.15.4 Telephone Line

If the telephone line is not working, the Technician may proceed to hand over the ATM to the Bank, but may not switch it 'live' or 'on-line'⁶.

2.15.5 Secure Area

ATMs should be stored in a secure area with reasonable restrictions on physical access, and with an access control procedure in place for all persons entering the area. Access control records should be kept for a minimum of two years, for external audit purposes.

2.15.6 Alarm System

The secure area should be protected by a monitored alarm system with sensors covering the external access points and all movement within the general area. This system should be switched on and monitored, outside of normal working hours, and at any time when the storage area is left unattended.

⁶ For Warranty purposes ATM Manufacturers require an on-line transaction to be completed

Chapter Three

Physical Security for Street-Based ATMs Against Ram Raids

3.1 Scope & Definitions

The scope of Chapter Three is limited to the security of 'street-based' ATMs in public telephone kiosks and columns/pods typically situated on public footways. Unless otherwise stated the advice contained in this document relates to both ATMs in telephone kiosks and in columns/pods.

The security guidelines listed are recommended as crime reduction good practice and the assessed risk will determine which, how many, and in what combination, these security measures may need to be employed.

Telephone Kiosks

With the advent of the mobile telephone in recent years the use of public telephone kiosks has significantly reduced.

In order to optimise the efficient use of these existing structures a number of ATM deployers have developed an innovative business model to utilise telephone kiosks as ATMs. Telephone kiosks offer a combination of three features that make them ideally suited for conversion to ATMs - publicly convenient locations, electricity and communications.

Columns/Pods

These are stand-alone structures of varying shapes and dimensions that house an ATM and in some locations Web/Internet connection facilities. These structures have typically been situated in car parks and other open locations to which the public have access and, more recently, on public footways.

3.2 Risk Assessment

The risk assessment will indicate what level of security is appropriate to the location for the street-based ATM. It will also help the deployer to decide which security measures need to be employed as well as in what combination these measures should be used.

3.3 Installation

3.3.1 Anchorage

The street-based ATM should be securely fixed to a specifically designed anchoring system or concrete base through its security container by a minimum of four high tensile M16 bolts with appropriate washers of 6mm minimum thickness. When fixing into a concrete base it is recommended that these bolts should be to a minimum depth of 150mm and that either resin anchor bolts or expanding anchor bolts are used to adequately anchor into the concrete.

3.3.2 Location/Position of Street-based ATM

The street-based ATM should be positioned in a highly visible, well-lit area that provides maximum casual surveillance by the general public.

In the case of columns/pods, the ATM should be positioned to take advantage of any existing street furniture such as railings, high-rise kerbing, raised planters, lamp posts, etc., which may offer a deterrent against ram-raid type attacks.

3.3.3 Closed Circuit Television (CCTV)(Optional)

Ideally, the street-based ATM could be located in an area where a public CCTV system operates.

When an ATM is located in an area where a public CCTV system operates, the deployer or agent should liaise with the agency responsible for the CCTV system to include the ATM site in any preset automatic camera settings or to request regular sweeps of the site.

The CCTV system should not be able to view the ATM keypad thereby preventing observation of PIN entry.

3.4 Recommended Security Measures

3.4.1 Safe

The security provided by the security container (safe) within the ATM should be to a level commensurate with that required for the value of cash contained therein. Reference should be made to the relevant EN 1143-1 or UL 291 ATM security standards.

3.4.2 Sounders and Flashing Warning Lights

The street-based ATM should be installed with an audible alarm sounder and/or visual flashing warning light to indicate when the ATM is under attack and attract the attention of the public and assist police in positioning the exact location of the ATM.

The sounder and/or warning light should be automatically disarmed during replenishment and servicing and automatically re-armed when replenishment / servicing is complete

3.5 Recommended Additional Security Measures for Higher Risk Deployments

Following a risk assessment, attain the security level required for the risk by deciding which, how many and in what combination the following security measures need to be employed.

3.5.1 Bollards

In addition to the anchoring system recommended in item 3.3.1, approaches to the ATM should be protected by the installation of anti-ram raid bollards, vehicle arresting systems, high-rise kerbing, raised planters, reinforced lamp posts or similar street furniture. These will usually be subject to local authority planning authority.

3.5.2 Enhanced Anchoring

In addition to the anchoring system recommended in item 3.3.1, the ATM should be secured with a restraining chain that is bolted to the anchoring system using a high tensile anchor fixing, connected through the rear of the ATM and attached to the security container using a high tensile bolt with double nut and washer.

3.5.3 Banknote Degradation System

A banknote degradation system may be deployed to protect each ATM cassette that holds banknotes contained in the ATM and provide a deterrent to theft of or from the ATM.

These systems provide a deterrent to theft and safety of operatives while transporting the cassette from the vehicle to the ATM, and during the replenishment or servicing.

Where a banknote degradation system is deployed, notices to this effect should be displayed prominently on the replenisher's vehicle and on the cassette itself or the container in which it is transported.

The banknote degradation system should be designed to activate immediately the ATM is moved or attacked by any means.

Where a banknote degradation system is deployed notices to this effect should be displayed prominently on the telephone kiosk, column/pod and on the ATM itself. Notices displayed where no banknote degradation system is deployed is crime reduction bad practice.

3.5.4 ATM Alarm System

The street-based ATM should be installed with an alarm system with its own unique reference number (URN). The system should be monitored using remote signaling to an Alarm Receiving Centre and should qualify for Level 1 police response. The design should ensure that the system is alarmed at all times other than for replenishment and servicing. Furthermore, it should give the earliest possible warning of attack on the ATM.

3.5.5 Tracking System

The street-based ATM should be fitted with a tracking system to enable its position to be determined in the event of the theft of the ATM.

Addendum Recommended Lock Types

For general guidance purposes for lock upgrades in the field, the following lock types are recommended for all installed ATMs:

Primary Safe Locking	<p>The following locks are recommended:</p> <p>A UL 437/Type 2, CEN Class B changeable key lock A 3 wheel UL Group 2M/ CEN Class B Mechanical Combination Lock A UL Type 1/ CEN Class B, 1 Time Code Electronic Combination Lock: in the event that this type of lock be used it is highly recommended that the following features should be taken into consideration:</p> <ol style="list-style-type: none"> 1. Lock should support encryption technology for the codes 2. Unused lock codes should expire automatically 3. Seal code should start a security protection procedure in the event that the previous ATM closing has not been correctly effected 4. Lock should be able to provide Shared access between the Bank and the CIT company autonomously and simultaneously 5. That the owner of the lock can at any time be able cancel access to the ATM lock park without having to organise on site vendor meets <p>A UL Type 1/ CEN Class B Electronic Combination Lock If applicable, the electronic locks should be compatible with the monitoring/control system used by the Bank/ATM deployer.</p>
-----------------------------	---

Secondary Safe Locking (For dual control if required)	<p>Where a mechanical 3-wheel combination lock is already in use, for the purposes of dual control an additional changeable key lock may be installed as a secondary lock to the primary. (A key locking dial may not be acceptable, dependent upon the agreed insured value for loss). Many modern electronic combination locks have a dual control function that allows dual control without the necessity to fit a second lock...</p>
One Time Combination Locks (For Use With Approved Third Parties if required)	<p>An approved third party is a commercial organisation authorised to carry cash in transit, to conduct cash replenishments and/or to conduct first & second line maintenance of the ATM. When such parties are used, it is recommended that one-time combination locks, with clearly identifiable audit trails, be used. Such locks may be used as the Primary Safe lock.</p>
Time Delay/Time Locks	<p>When required a programmable time delay lock may be fitted, allowing a pre-set delay whenever the lock is opened., this is usually 1-99 minutes in 1 minute increments Such a Lock, which may also be used as the Primary Safe Lock, may also be programmed as a Time Lock, whenever the Bank Branch/ATM Site is closed, and between replenishments.</p>
Time Delay Override (TDO)	<p>In the event that a Multiple/Dual User Electronic Lock is fitted, it should be able to be programmed with a Time Delay Override Code (TDO) that can be used by the CIT or ISO to allow the user to by pass the time delay for obvious reasons. The TDO should be able to be programmed to either allow direct after hours entry or Dual entry (second code needing to be entered within 60 seconds of the first)</p>
Duress Alarm (Hold Up alarm)	<p>The electronic lock should also be able to generate a "Duress" alarm. It is advisable that this code be easy to remember and use and not require any</p>

	additional keystroke to activate. The best is 1 code up 1 code down activation; meaning if the code was 123456# the user would substitute the last digit by either a number above or below that of the last digit.
BPI (Bolt Position Indicator)	Electronic locks should also be able to provide a dry signal indicating if the bolt is in the Retracted position (open) or the Extended (Closed) position. This signal can be used to monitor the condition of the lock remotely, prevent a cascade (multiple door openings at the same time) attack on a group of ATMs or freeze the entry to the ATM room in the event that an ATM door is in the open condition. Alternatively there are many safe alarm systems in operation that monitor bolt position by other add-on means and these are acceptable and even compulsory alternatives in some countries.

Some Reported Successes

The Ram Raid Committee of GASA will keep an updated list of reported successes in employing security technologies and strategies which have led to a noticeable reduction in the incidences of ram raids. Please send submissions to Mike Lee at mike@atmia.com. The difficulty is always the ROI/expense for the deployer who carries out a cost-to-benefit ratio analysis in terms of typical losses suffered. *These security devices are not ranke din any order of importance or effectiveness.*

1. Installation of a **GPS device** that can send signals from deep inside buildings.

Rationale for Method

Deployers can track the stolen machines before they are forced open.

The thieves can then be caught red handed – resulting in a decrease in thefts of ATMs.

2. Use of **banknote degradation systems**⁷.

Rationale for Method

A banknote degradation system should be deployed to protect each ATM cassette that holds banknotes contained in the ATM and provide a deterrent to theft of or from the ATM.

The banknote degradation system should be designed to activate immediately the ATM is moved or attacked by any means.

Where a banknote degradation system is deployed notices to this effect should be displayed prominently on the telephone kiosk, column/pod and on the ATM itself. Notices displayed where no banknote degradation system is deployed is crime reduction bad practice.

3. Use of **Anti-lasso device**.

Rationale for Method

These physical devices are used when the back of the ATM does not fit flush to the wall due to skirting of other reason. These devises generally consist of a metal bar attached to the top of the main body at the back of the ATM that extends to the wall and sidepieces that are bolted to the side fascias to fill any gap between the ATM and wall. These devices are used to prevent chains, crane straps or similar objects being easily placed behind the ATM in preparation to rip the ATM from its anchoring.

⁷ Bank note degradation systems may be linked to an end-to-end solution for maximum effectiveness.

4. Use of **bollards**.

Approaches to the ATM should be protected by the installation of anti-ram raid bollards, vehicle arresting systems, high-rise kerbing, raised planters, reinforced lamp posts or similar street furniture. These will usually be subject to local authority planning authority.

Rationale for Method

To prevent hostile approaches from vehicles to the ATM and the premises where it is located, thus reducing the risk of ram raids and the effectiveness of any attack using vehicles.

5. Use of **ATM Plinths**.

Rationale for Method

Specifically designed ATM plinths can provide additional security against ram raids and other brute force attacks. However, the ATM must be properly fixed to the plinth with a minimum of four anchor points and the plinth should be secured to the floor by not less than six anchor points to ensure resistance against forcible attack.

6. Use of **Chains**.

Rationale for Method

The ATM should be secured with a restraining chain that is bolted to the anchoring system using a high tensile anchor fixing, connected through the rear of the ATM and attached to the security container using a high tensile bolt with double nut and washer.

Chains are used to provide additional anchoring protection against ram raids and to delay in-situ attacks against ATMs; dependent on the quality of the chain used these can also provide anti-cut properties.

7. Use of **CCTV**.

Rationale for Method

As a deterrent and as a tool for capturing evidence against suspects.

8. Use of **Sounders and Flashing Warning Lights**.

Rationale for Method

The ATM should be installed with an audible alarm sounder and/or visual flashing warning light to indicate the ATM is under attack and attract the attention of the public and assist police in positioning the exact location of the ATM.

The sounder and/or warning light should be disarmed during replenishment and servicing.

9. Use of **Enhanced Anchoring**.

Rationale for Method

Enhanced anchoring systems should be used for higher risk ATM installations to protect against ram raids or rip-outs. These systems generally allow a degree of movement when attempting to forcibly remove the ATM and prevent purchase being gained in any one direction.

10. Use of **ATM Alarm System**.

Rationale for Method

The ATM should be installed with an alarm system with its own unique reference number (URN). The system should be monitored using remote signalling to an Alarm Receiving Centre and should qualify for Level 1 police response. If it is a 'confirmable' alarm system, a dual signalling facility should be provided.

The design should ensure that the system is alarmed at all times other than for replenishment and servicing. Furthermore, it should give the earliest possible warning of attack on the ATM.

Acknowledgements

1. Alan Townsend, ATMIA European Security Adviser
2. The ATM Security Working Group, Chaired by Alan Townsend, ATMIA European Security Advisor "STAND-ALONE" ATMs - RECOMMENDED SECURITY GUIDELINES", published September, 2002 and "STREET-BASED ATMS- - RECOMMENDED SECURITY GUIDELINES" published September, 2004
3. Recommended ATM Security Guidelines ("Wall Mounted" ATMs)", by Lachlan Gunn, launched November 2003
4. The Ram Raid Committee, Global ATM Security Alliance
5. Graham McKay, Executive Director, ATMIA Europe
6. NCR's ATM physical security experts at NCR's head office in Dundee

Disclaimer

This manual has been developed in furtherance of GASA's and ATMIA's non-profit purposes. The information contained in this manual is intended to identify Best Practices in the ATM industry, but is not a standard for best practice. Therefore, use, reference to, or review of the material in the manual does not and cannot guarantee the elimination of risk inherent in the delivery of ATM services and should not be used as a standard or mandatory requirement for conducting business in the ATM industry. It is recommended that the manual be used as guidance in connection with the implementation of Best Practices, but not as a substitute for diligent review and analysis regarding application of the Best Practices.

GASA and ATMIA have taken reasonable measures to develop the manual and recommended Best Practices in a fair, reasonable, open, and objective manner. However, GASA and ATMIA make no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information being provided. In addition, views of appropriate practices may change over time and errors or mistakes may exist or be discovered in this material. As such, inclusion of material in this manual does not constitute a guarantee, warranty, or endorsement by GASA or ATMIA regarding the views, methodologies, or preferences for implementing the Best Practices. Further, neither ATMIA nor GASA nor its officers, directors, members, authors, or agents shall be liable for any loss, damage, or claim with respect to any such information or advice being provided. All such liabilities, including direct, special, indirect, or consequential damages, are expressly disclaimed and excluded.