Security

Cash Security: A User's Guide

S22
First published 2013
Version 01

RISCAuthority

administered by FPA Fire Protection Association

IMPORTANT NOTICE

This document has been developed through the RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

The FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, the FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, the FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, the FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

CONTENTS

1.0 INTRODUCTION

1.1 Purpose of this guide

Cash is especially attractive to criminals and, particularly where held/handled in significant quantities, is often the object of sophisticated attempts at theft (burglary or robbery). This guide has therefore been produced to assist organisations handling significant amounts of cash, as part of their everyday business, to assess and control the risks to which they are exposed.

For basic guidance on protecting smaller amounts of cash from robbery reference can be made to another RISCAuthority guide: S19 **Security Guidance for defence against robbery**. This guide – and others listed below, which may provide further useful information – is available from the RISC Authority website: www.riscauthority.co.uk

S3 **Convenience ATMs - Recommended security measures**

S6 **Electronic Security Systems - Guidance on keyholder selection and duties**

S7 **Security fog devices**

S9 **Intrusion and hold-up alarm systems (I&HAS) Considerations for installers and other stakeholders**

S10 **Guidance for the protection of premises against attacks using vehicles (ram raids)**

S12 **Police response to intruder alarms systems: ten-step guide for purchasers**

S17 **Intrusion and hold-up alarm systems: guidance on event processing and handling**

S20 **Essential principles for the security of property**

1.2 Scope

The guide is focussed upon the potential for a significant degree of loss arising from the criminal actions of third parties, but does not extend to address other risks such as: theft by employee; theft by fraud or theft by electronic means. Exposures addressed in this document include cash on the premises during working hours, cash on the premises out of hours and cash in transit.

For the purposes of this document a significant degree of loss is deemed to be one where there is the potential for the theft of cash in excess of £30,000 e.g. larger retailers, cash and carry outlets, visitor attractions, exhibition centres, sports stadia, cash centres, casinos, bureaux de change, banks, building societies and the like.

Although 'cash' is typically considered to be notes and coins, the guide is equally relevant to significant exposures of vouchers, stamps, bankers' drafts and other negotiable instruments.

This document presents only the general principles of managing cash handling exposures. Where further detailed guidance or approval of proposed measures is required the reader should refer to their insurance company.

1.3 Risk and insurance

When reviewing cash security measures, it is important to be aware of the extent and detail of any conditions applicable to any related insurance cover in order to avoid the risk of unwittingly undermining them. Examples are conditions such as those relating to key security, use of an intrusion and hold up alarm system (I&HAS), cash carrying precautions, money in vehicles etc.

1.4 Staff safety

Aside from the risk of money theft, an organisation is obliged by the Health and Safety at Work Act to provide a safe place of work and safe systems of work. It is also obliged to undertake risk assessments and provide adequate training and instruction for employees, all of which should be fully documented.

2.0 MANAGEMENT PROCEDURES

2.1 Security policy and manual

There should be a clear policy defining roles and responsibilities and also the safe working procedures in place to manage the cash risk. A security manual should be maintained detailing the security policy and the various specific measures and procedures to be employed in its support, such as: access control arrangements; locking and unlocking procedures; security equipment and systems; key and code control; security personnel selection and incident management.

2.2 Staff recruitment

The staff recruitment process should ensure that all new staff (including temporary and agency staff) are subject to rigorous checks; including identity verification, a Criminal Records Bureau (CRB) check and verification of employment history.

The licensing requirements of the Private Security Industry Act must be observed with regard to any staff directly employed in licensable roles (e.g. door supervision in licensed premises) and all contractor supplied manned security personnel. An initial step in ensuring that contractors are observing Security Industry Authority (SIA) licensing procedures is to only select those companies who hold National Security Inspectorate (NSI) or Security Systems and Alarms Inspection Board (SSAIB) accreditation for guarding activities or otherwise ensure that they are at least members of the voluntary SIA Approved Contractor Scheme (ACS).

2.3 Staff training

All staff involved in security roles should receive generic and site specific training in accordance with the procedures laid down in the security manual.

2.4 Operational procedures

Opening and closing procedures should be well defined and documented for both the working day and also customer access hours and should always involve at least two persons. Persons assigned premises unlocking and locking duties should not include those who have the means to unlock safes, vaults, ATMs or other cash containers. Entrance doors should remain locked until customer trading hours commence.

Calls purporting to be from an alarm receiving centre (ARC), the police or some other authority requesting keyholder attendance should be validated by ring-back to known (pre stored) numbers.

An access control system should be installed which restricts access to sensitive areas such as cash offices, cash transfer bays/routes and security control rooms, to those personnel with appropriate jobholder responsibilities only.

2.5 Contractors and visitors

Contractors and visitors (other than walk in customers whose business can be transacted within customer-access areas) should only be received:

(i) by prior appointment

(ii) with appropriate management authority

(iii) subject to identity verification upon arrival.

They should then be signed in and out, wear visible badges and, ideally, be accompanied at all times.

3.0 PREMISES RISK: BUSINESS HOURS

Every attempt should be made to keep cash exposures in customer facing areas as low as possible and to move excess sums to a better defended location well away from the 'shop floor'.

3.1 Cash and wages offices

For operational as well as security reasons, cash accumulations are frequently best managed within a single office or suite located well away from areas where the public have access, preferably on an upper floor.

The cash room should be built to at least a 'manual attack resistant' (formerly referred to as 'anti bandit') specification. Where the assessment indicates that there is a reasonably foreseeable threat of firearms, threat facing elements of construction (including glazing) should be of bullet resistant standard.

In a cash office incorporating a customer interface point (e.g. a transaction counter), the design should include a 'safe haven' retreat for cashiers. Wherever possible, access into the cash room should be via a security lobby comprising a pair of 'in series, interlocked' security doors. The cash room should be equipped with hold-up alarm buttons.

3.2 Access control

The access control policy should establish the levels of authority for access to cash sensitive areas and the means of controlling this access.

In practice this will generally require the use of both (i) an electronic access control system and (ii) an operational procedure that relies upon authorised staff within the cash room positively identifying the person(s) seeking admission and unlocking the access door(s) for them (either directly or remotely).

3.3 Security control rooms

Heavier risks will warrant a level of surveillance and security management that may necessitate the establishment of an on site security control room from which security personnel can supervise the premises from a location that is itself well secured against criminal attack. The room should be to the same standard as a cash office and equipped with:

- CCTV management systems
- alarm annunciation equipment
- access control system event alert facilities
- on site and off site communications equipment
- hold-up alarm buttons

3.4 Hold-up alarms

A hold-up alarm system should be installed where the cash risk is significant. To avoid false alarms and the related risk of withdrawal of police response, staff should be provided with full training. The hold-up alarm should be silent at the location and the deliberately operated devices used to activate it should be distributed and positioned such that they can be readily accessed and operated discreetly.

In addition to sending a hold-up alarm notification to the ARC, any activation of a hold-up alarm device should ideally also register a discreet alert to senior staff at the location, away from the immediate threat area so that they can activate the hold-up contingency plan detailed in the company security manual. Refer section 4.6 for general intruder alarm requirements.

3.5 Duress Alarms

For very heavy cash risks, consideration should be given to the possible need for duress alarm facilities to be incorporated into electronic security systems such as the premises I&HAS and perhaps also any supervised digital locks on cash safes or strongrooms so that a member of staff unsetting an alarm or unlocking a safe or strongroom under duress can comply with the assailant's instructions whilst at the same time sending a discreet duress signal to an ARC (and/or the in house security control room).

IMPORTANT NOTE. A duress facility is only permitted by current police policy if certain stringent technical standards are met. A special application may need to be made – the alarm company can assist.

3.6 Cash in safes

Cash that is not required to be immediately available to cashiers and other staff (i.e. in tills) should ideally be kept in locked safes in secure, staff-only areas and, for any safes holding significant sums, only in areas to which designated staff (e.g. cashiers and/or managers) have access. Safes should never be positioned in locations to which the public have access. They should be kept locked at all times other than when it is necessary for the safe door to be opened for purposes of removing or depositing cash in the course of normal business operations.

A time delay lock, especially where its presence is advertised, will provide an additional deterrent to criminals contemplating a day time raid. The programmed delay has to strike a balance between operational convenience and providing effective security. It should be no less than 5 minutes, and may need to be significantly greater as cash values at risk increase, e.g. police often recommend a programmed delay of around 20 minutes. An alternative compromise solution is sometimes found with the use of a safe 'coffer' built in, or retro fitted, within the safe which is used to contain the bulk of the cash, and is fitted with the time delay device whilst 'on-call' cash is left outside the coffer, although still within the locked safe.

It may be advisable to install a 'deposit safe' so that the person responsible for cash receipts can 'post' them into the safe without opening the safe door, and thus need not be issued with a key, combination number or PIN. As with time-delay devices, good signage notifying potential raiders of the fact that staff do not have the means to open the safe, will help to maximise the deterrence value.

Safes must be of adequate quality for the value being held and should not exceed any cash limit set by an insurer's policy (see section 4.2).

3.7 Cashier counters

Where required these should comprise a proprietary cashier window with in-built transaction tray (preventing line-of-fire access beneath the screen). Where transactions include the passage of large bags, a proprietary cash transfer hatch or hopper to the requisite resistance level should also be provided.

As an alternative to fixed screens, 'open' counters may be constructed to incorporate fast rising (normally bullet resistant) screens, activated by staff.

3.8 Till points

Should ideally be positioned away from external doors and with strict cash limits applied. Secure transfer systems should be considered (e.g. vacuum tube/air pressure transfer) or a procedure employed to 'bleed' (siphon off excess cash) tills at regular intervals during trading. An alternative is the use of at-till or local-to-till secure deposit facilities, whereby staff can post surplus receipts into a robust, anchored container the keys to which, for the purposes of removing deposits, are held by other, non-front-line staff, or by a contracted CIT firm.

3.9 Cash transfers within the business premises

Automated point-to-point delivery systems (for example those based on localised air pressure tube installations) generally offer the safest and most secure means of transferring cash between cash office and cashier/till operator.

Staff accompanied cash transfers within the premises during business hours should be designed to take the safest (not necessarily the shortest) route, avoiding potential high risk areas. Cash transfers can be transported within a proprietary (or otherwise purpose designed) cash trolley incorporating attack resistant cash container(s) or, if the weight of cash to be transferred is not great, in cash bags. A wide variety of bags is available ranging from simple cotton coin bags to alarmed cases to security bags equipped with smoke-and-dye packs (selection depends upon the amounts of cash being transferred and its vulnerability).

3.10 Additional hold-up defences and deterrents

3.10.1 CCTV

All significant cash risks should include continuously recorded (minimum 25 frames per second) CCTV designed to ensure that all customers and visitors are aware of its existence upon entry to the premises and that camera coverage is comprehensive. The recorded image quality should be of sufficiently high standard for criminal evidence personal identification purposes with clear, high resolution head-and-shoulders images available from at least one camera of all persons entering or leaving the premises.

Camera placement should ensure good coverage of all external doors (internal and external views), customer access areas, cashier counter/till positions, cash office and security control room (interiors, entry doors and approaches).

3.10.2 Security fog systems

During working hours this can be cashier activated, using deliberately operated devices (normally personal attack buttons). Anti raid security fog systems are designed to 'push' the attackers away from the cashiers' counter and back towards the street entrance door. It is important to be satisfied that any installation proposed will perform sufficiently rapidly and effectively to meet this specific operational requirement. There are various issues to be considered when installing such a system so close liaison with the insurer is essential.

3.10.3 Forensic coding (unique tagging) spray systems

The system may be configured to discharge its spray in reaction to both a hold-up alarm (i.e. a cashier activated personal attack button) and an intruder alarm (i.e. activation of a detection device when the alarm is set). In the case of the former, the spray would normally be discharged around anticipated raider escape routes (e.g. the front entrance door to a high street bank). As with security fog systems, it is important that all staff are fully trained in the appropriate use of the system and have the opportunity to witness a test or demonstration discharge.

3.10.4 Bank note degradation and unique tagging systems

Automatically detonated dye packs may be inserted into 'dummy' stacks of bank notes within cashiers' cash drawers. These particular stacks are intended only to be handed over in a raid situation and the system is designed to permanently mark all the stolen bank notes with a strongly coloured dye rendering them unusable for normal transactions. The dye may additionally include unique tagging properties to link the perpetrator to the crime for evidence purposes.

3.10.5 Signage

Central to the aim of deterring attempts at robbery is the need to ensure, as far as possible, that potential raiders are aware that their chances of achieving a successful, lucrative crime are very low. There should thus be prominent signage at each public entrance to the premises indicating in brief and easily understood terms the range of security measures deployed.

4.0 PREMISES RISK: OUT OF BUSINESS HOURS

When the premises are closed for business, all cash should be locked away in suitable containers. In the vast majority of cases, this will mean that all (or virtually all) cash should be placed in locked safes or strongrooms.

4.1 Premises security

External doors should be of robust construction - particularly those in more secluded, vulnerable positions such as at the rear of the premises. Accessible windows and glazed panels in external doors should be protected with steel security grilles, with the possible exception of those at the front of the building where natural surveillance may render a surreptitious intrusion attempt less likely.

If the premises are protected by on site security guards out of business hours it is important that they have no means to access (even under duress) any part of the building containing cash, or any other sensitive areas. It is also imperative that their presence is backed up by an appropriate, remotely monitored intrusion and hold-up alarm system and that their presence on site does not in any way restrict the coverage or hinder the operation of the system. In particular, ideally they should not be able to unset it.

4.2 Safes

For significant cash exposures, the only safes likely to be sufficiently robust are the higher rated free standing (i.e. floor standing) units, although some of the highest quality underfloor safes might be accepted in some circumstances for moderately high cash limits. Wall safes are unlikely to be considered to offer adequate security.

4.2.1 Resistance 'grades' and overnight limits

Cash safes, ATM safes and strongrooms should only be selected if independently tested and certified by a recognised certification body as having achieved a particular attack resistance level ('grade') as defined in a recognised standard, e.g. BS EN 1143-1 Secure storage units - Requirements, classification and methods of test for resistance to burglary - Safes, ATM safes, strongroom doors and strongrooms, or BS EN 1143-2 for deposit safes. The 'grade' will determine nominal 'out of hours' cash limits, which will need to be confirmed by your insurer.

4.2.2 Location and fixing

Forcible opening of a high quality safe is a more favourable proposition for the safe-breaker if the unit can be uplifted and removed to a location where it can be attacked over a prolonged period without risk of discovery.

The importance of location and fixing is dependent on the location of the safe and its size. Whilst all freestanding safes should be anchored in accordance with the manufacturer's recommendations, it is generally an imperative for safes weighing less than 1,000 Kg.

4.2.3 Locking arrangements

The minimum number and quality of locks required is specified within BS EN 1143-1 according to 'grade' of safe (e.g. a minimum of one EN 1300[1] Class B lock for a 'grade' 3 safe). All safes 'graded' 4 and above must be fitted with a minimum of two locks and, depending on 'grade', these locks are required to be Class B, C or D.

If the whereabouts of any key (either supplied originally or as an additional copy) can not be ascertained, the safe lock(s), lever set(s) or equivalent, must be replaced by a competent safe specialist and the replacement keys assigned to the nominated keyholders.

Safe keys must be retained in the custody of senior, authorised personnel and be removed from the premises when they are left unattended.

Mechanical combination locks and electronic PIN locks overcome the main risks associated with key locks (i.e. loss or theft) but introduce other potential problems. It should thus be ensured that the combination number is made available to the minimum number of suitably authorised personnel only (one PIN number per authorised user in the case of electronic locks), that it is not recorded anywhere in writing or electronically and that the number is changed routinely (e.g. every 6 or 12 months) and every time that a 'keyholder' leaves employment or a breach in security is suspected.

Any safe that is required to hold significant amounts of cash (whether or not it is a modern 'BS EN graded' safe) should be equipped with at least two locks with two persons required to be present in order to unlock it.

The risk of losses through duress and kidnap out of business hours can also be reduced by the use of a safe time lock. The time lock should be set to permit opening of the safe door only during normal working hours.

A wide range of electronic safe locks is now available offering a multitude of different functions including allocation and deletion of individual PIN codes, deployment and adjustment of time-locking and time delay functions and event audit trail.

For risks with multiple locations it is also possible to fit remotely managed electronic locks so that the various adjustable functions and parameters may be configured over an entire estate of safes, audit trails may be viewed from a central location and event alerts or exception reports (e.g. safe remaining open after set time) can be transmitted to a security manager or response officer. Such remote functionality must, of course, not extend to allow any 'unlock' commands.

[1] EN 1300 - Secure storage units. Classification for high security locks according to their resistance to unauthorized opening

An optimum solution can sometimes be found by twinning a modern electronic lock with a traditional high security mechanical key lock, with both devices in use out of business hours.

4.2.4 Deposit safes

Safes with inbuilt cash deposit facilities can be specified to good effect with the intention of minimising the risk of hold-up and this should be emphasised by clear and concise signage at the point of threat. Deposit facilities should be of the type built in by the manufacturer and independently tested and certified in accordance with BSEN1143-2 (Deposit systems).

4.3 Strongrooms

Where the physical volume of cash (and/or other valuable property) at risk is such that cash safes would be incapable of providing sufficient capacity, strongrooms can offer a viable alterative.

Modern products tend to be of the 'demountable' (pre-fabricated and assembled on site) type rather than the more traditional 'built in situ' strongroom or vault and, like cash safes, they should be independently tested and certified against BS EN 1143-1.

4.4 Automatic Teller Machines (ATMs)

ATM safes (the 'safe' type compartment within ATMs) certified by recognised certification bodies to EN 1143-1 may reasonably be considered as deserving of similar out-of-hours cash limits as are safes of similar 'grade', provided that the positioning and anchoring of the ATM are satisfactory (particularly in light of the number of ram raid attacks on through-the-wall and even, lobby, ATMs).

ATMs certified to UL 291 may be classified as 'business hour service', Level 1 or Level 2 and, of these, it is considered that only the highest class (Level 2) approximates in resistance terms to a mid-range cash safe. Indeed, 'business hour service' ATMs are not intended (even by their manufacturers) to hold cash out of business hours.

All ATMs should be securely anchored to the structure of the building, preferably to a concrete floor, in accordance with the manufacturer's recommendations, and be alarm protected to a high standard. Fogging systems may also be employed.

ATM cash replenishment should preferably be undertaken by operatives from a contracted professional Cash and Valuables in Transit (CViT) company.

4.5 Other customer interface and cashier support machines

There are, in today's financial, leisure and retail sectors especially, a host of cash-handling, receiving, recycling, changing, gaming and vending machines installed in publicly accessible areas for direct use by customers. Few of these machines offer much resistance to violent attack so emptying machines and advertising the fact (with signage and leaving the empty cash containers unlocked and doors ajar) can sometimes save significant losses. Where significant cash exposures (per unit or in the aggregate) will remain in machines out of business hours it is important to seek your insurer's advice.

4.6 Intruder alarm and CCTV protection

All out-of-hours cash exposures of any significance should be intruder alarm protected to a high standard. The system should be to at least Grade 3 of BS EN 50131-1 - Alarm systems - Intrusion and hold-up alarm systems with Level 1 police response. It should incorporate a dual path alarm transmission system (ATS) suitable for use with EN 50131-1 compliant systems up to and including security grade 4, notification

option C, i.e. with a performance level of ATS5 (ideally independently tested and certified e.g. as per the LPCB's LPS1277 3.0 scheme).

The system design should ensure that a confirmed alarm will be generated before intruders reach any cash safes, ATMs or other cash containers within the premises. In addition to protecting normally envisaged access points (doors and windows) and routes, consideration should also be given to the possibility of intrusion through walls or floors, particularly from any neighbouring vacant properties.

Set and unset signals should be monitored by the ARC for compliance with notified closing and opening time windows, and any deviations (for example failure to set, or out-of-hours/early unset) should be immediately notified to the duty keyholders.

Safes, strongrooms and ATMs holding significant amounts of cash should be additionally protected with safe 'limpet' or vault-guard detectors on a 24-hour circuit as an added defence against in house thefts, collusion, alarm system compromise by masking movement detectors, etc.

Consideration should also be given to protecting the room or compartment containing the ATM with suitable shock sensing detectors so that so that any attack from outside the alarm protected portion of the premises will also be detected.

Vending, ticketing and other cash holding machines that are installed in the open (e.g. in car parks, on station platforms or public pavements) should also be alarm protected against violent attack, unauthorised opening of the casing or access doors and removal, and preferably with both local alarm sounder and network borne alarm signal.

All ATMs and other machines holding, receiving and dispensing cash in publicly accessible places should also be supervised by CCTV systems with 24-hour recording facility as a minimum and preferably also alarm activated real time monitoring.

4.7 Security fog systems

Security fog systems can be used to very good effect in protecting business premises against out-of-hours theft losses (see 3.10.2).

4.8 Bank note degradation and unique tagging systems

As an added deterrent safes, ATMs and other (bank note) cash containers may be fitted with automated bank note degradation and unique tagging systems (see paragraph 3.10.4) activated by attack-sensing devices mounted within the unit. In addition to the familiar 'smoke and dye' note marking materials, systems are now available that aim to render stacks of bank notes unusable by the use of an adhesive to solidify them and prevent non-destructive separation.

5.0 EXTERNAL TRANSITS

The transportation of significant sums of cash is a potentially hazardous process which is best undertaken by well trained and properly resourced professionals, rather than as an ancillary part time function by in house staff. Health and Safety considerations alone should be sufficient to persuade most businesses with significant cash in transit needs to employ the services of a professional Cash and Valuables in Transit (CViT) carrier.

5.1 Professional carriers

Professional CViT services should ideally be used for all transits of cash to and from the business premises and, when amounts in transit represent a sizeable target for criminals, the use of such services becomes vital. To ensure that the CViT contractor complies fully with the current edition of BS 7872 Manned security services – Cash and valuables in transit services (collection and delivery) Code of practice, select a company approved by the National Security Inspectorate (NSI). If the preferred contractor is not approved under the NSI scheme, it should be ensured that it is at least listed under the voluntary Security Industry Authority's Approved Contractors Scheme (SIA-ACS).

The contract will probably, amongst other things, set limits on the maximum amount of cash per consignment (and per single cash bag), so it is important that management procedures, standing instructions and staff training programmes ensure that such limits are adhered to and that other contract terms continue to be met.

Attention must be paid to the arrangements for cash transfer at the premises. In particular, use of an estimated time of arrival (ETA) notification procedure; provision of a safe and secure environment for the transaction; provision of a safe and secure route from the cash office; and strict adherence to documented procedures.

5.2 Transits by own staff

The maximum amount of cash in transit per consignment should be agreed with any insurer with particular reference to any requirements the insurer may make. There may, in consequence, need to be an increased number of transits in order to meet the cash flow needs of the business and to avoid exceeding insurance policy limits.

Cash transits should be subject to full risk assessment and transits should always be accompanied by at least two members of staff and preferably more. Significant sums will often warrant 3 or 4 persons to accompany the cash.

Transits by staff should be as discreet as possible with times, routes and amounts known only to a minimum number of responsible personnel and with care taken to avoid, as far as possible, identifiable and predictable routines. The closest bank may not always offer the safest route.

It is preferable for cash to be carried on the person (e.g. in pockets) where it is practicable to do so, dividing the consignment between the escorts as necessary in order not to draw attention unnecessarily to the purpose of the journey. Where the volume of cash is such that bags have to be used, then these should be anonymous in appearance so that the nature of their content is not readily evident.

For significant sums in transit, proprietary cash-carrying bags (or alternatively security device bag-insert units) should be considered. Any vehicle used for the transportation of money should also be as anonymous as possible. The route should be planned so as to avoid quiet, isolated roads, there should be no other purpose in the journey than the delivery/collection of money to/from the bank and there should be no unnecessary other stops (e.g. for fuel). All doors, hatches and boot lids should be kept locked for the duration of the journey. The vehicle must never be left unattended when containing money.

Fire Protection Association
London Road, Moreton in Marsh
Gloucestershire GL56 0RH, UK
Tel: +44 (0)1608 812500 Fax: +44 (0)1608 812501
Email: administrator@riscauthority.co.uk
Website: www.riscauthority.co.uk

Hard copies of this document may be obtained from the
publications department of the FPA at the above address.

RISCAuthority

administered by FPA Fire Protection Association