S3
First published 2007
Version 02

Security

Convenience ATMs: recommended security measures

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. INTRODUCTION

The scope of this document is limited to the security of 'stand-alone' or 'freestanding' automated teller machines (ATMs), typically located in convenience stores, petrol stations, supermarkets, pubs and clubs. The guidance given within this document is designed to reduce the risk of crime occurring on premises where such ATMs are installed and outline the implications for insurance provision.

Associated documents:

- S6: **Electronic security systems: guidance on keyholder selection and duties**;
- S7: **Security fog devices**;
- S12: **Police response intruder alarm systems: ten-step guide for purchasers**;
- S14: **Police response intruder alarm systems: summary of insurers' typical requirements**;
- S10: **Guidance for the protection of premises against attacks using vehicles (ram raids)**;
- S16: **Guidelines for shop front protection**; and
- RISCAuthority guidance - 'Cash Security' (in preparation).

(These documents may be downloaded free of charge from the website: www.riscauthority.co.uk and those available in hard copy form may also be purchased from the Fire Protection Association.)

2. BACKGROUND

ATMs found in retail and other types of premises have either been supplied and installed by an independent ATM deployer (IAD), bank, building society or other financial institution. Usually the ATM has been supplied on a contractual basis between the supplier and the premises owner or occupier. There are two different types of contract in existence.

Contracts involve either:

- **Merchant Fill:** an ATM filled by the business operator, who owns the money in the ATM until it has been dispensed; or
- **Cash-in-Transit company (CIT Fill):** an ATM filled by the supplier, who owns the money in the ATM until it has been dispensed.

Under CIT Fill type of contract, the ATM supplier simply provides a service facility for the ATM and its operation. The consequences of theft of money from the ATM, and any damage to the ATM consequent to that theft, will normally be insured by the ATM supplier, as the supplier owns the money held in the ATM. However, in many instances, this cover does not extend to include any damage to the premises caused by that theft and this risk is normally borne by the insurer of the operator/occupier of the business/premises.

3. SECURITY GUIDELINES

The security guidelines that follow focus on the key issue of removal of an ATM from the premises – often following a ram raid, with the ATM being opened and the cash removed at a location remote from the scene of the crime. This type of incident invariably causes considerable incidental damage to the premises and, often, to its contents, resulting in cost.

The guidelines are designed to prevent or frustrate removal of ATMs as well as outlining measures that can deter or hinder attacks on them.

4. RISK ASSESSMENT

In order to determine the requisite level of security for the site and to assist in the choice of ATM contract (Merchant Fill or CIT Fill), a careful risk assessment should be made involving all interested parties (premises operator, IAD and insurer).

Such an assessment should take account of:

- the safety of all staff, ATM users, and the general public;
- the crime history of the area and the site itself;
- local police intelligence;
- the position of the ATM on site;
- cash replenishment procedures;
- existing security measures; and
- proposed site security measures.

In addition, when deciding whether a Merchant Fill or CIT Fill contract would be most appropriate, the individual circumstances of the business should be considered, together with its ability to comply with the recommended cash removal and replenishment provisions (see below) for Merchant Fill ATMs.

5. SECURITY RECOMMENDATIONS FOR ALL ATMs

Anchorage: 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 should then be bolted through the floor joists by a minimum of four bolts.

Location: The ATM should be sited within the premises well away from perimeter glazing, particularly shop fronts, and preferably directly against a substantially constructed internal wall or a substantially constructed perimeter wall which does not have vehicular access to its external face. It should also be positioned to avoid a direct and unimpeded line of access from a door or other access point.

Visibility: Notwithstanding the advice about location stated above, to reduce the risk of vandalism to the ATM and 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.

6. ADDITIONAL SECURITY RECOMMENDATIONS FOR MERCHANT FILL ATMs

- The ATM should be filled with cash sufficient for one day's trading only; the insurer will usually set a policy limit.
- At the end of trading hours, cash should be removed from the ATM to a safe of adequate security quality (as confirmed by any interested insurer) sited within the premises; this should be done with the premises locked and customers excluded.
- The door to the ATM, and the security container within, should be left open when the business is non-operational.
- Notices should be placed prominently around the perimeter of, and within, the premises stating that the ATM holds no cash when the premises are closed.
- Cash should be replaced in the ATM prior to the premises opening to the public for the next period of trading.
- In the event of an attack during opening hours, staff should be

advised to comply passively with the raiders' demands and they must be trained accordingly.

- Depending on the amounts of cash at risk and the general security risks of the premises, intruder alarm protection may also be advisable – see the relevant comments included under the additional security recommendations for CIT Fill ATMs.

Important: Merchant Fill ATMs are not security safes in the accepted sense and consequently have not undergone a performance standard test such as that required under BS EN 1143: **Secure storage units. Requirements, classification and methods of test for resistance to burglary** (various parts). As such, they have not been designed to sustain a determined physical attack and, consequently, if the business finds itself unable to comply with the cash removal and replenishment provisions listed above, it should only consider the installation and use of a CIT Fill type ATM.

7. ADDITIONAL SECURITY RECOMMENDATIONS FOR CIT FILL ATMs

- As agreed with any interested insurer, the premises should be protected by an intruder alarm system providing appropriate security/resilience, which typically would include remote signalling (via a monitored dual path alarm transmission system) to an alarm receiving centre able to request a police response. Any new system should be installed in accordance with BS EN 50131-1: 2006 + A1: 2009: **Alarm systems. Intrusion and hold-up systems. System requirements** and the scheme described in PD 6662: 2010: **Scheme for the application of European Standards for intruder and hold-up alarm systems**. The Grade of such a system and its notification (remote signalling) requirements will usually be indicated by an insurer in keeping with the assessed risk. Given the type of criminal likely to be attracted to locations with an ATM, a Grade 3 system will frequently be recommended with 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, ie with a performance level of ATS5 (ideally independently certified, for example as per the LPCB's LPS 1277 3.0 scheme).

  The system should be designed to give the earliest possible warning of attack on the ATM. Consideration should be given to providing personal attack devices linked to the system. Additional information and guidance may be found in RISCAuthority document S12: **Police response intruder alarm systems: ten-step guide for purchasers**.
- External approaches to the area of the premises where the ATM is sited should be protected by the installation of anti-ram bollards or similar, subject to local authority planning approval. Additional information and guidance may be found in RISCAuthority document S10: **Guidance for the protection of premises against attacks using vehicles (ram raids)**.
- Where perimeter glazing extends down to the floor of the premises, this should be protected by metal roller shutters outside of trading hours. Additional information and guidance may be found in RISCAuthority document S16: **Guidelines for shop front protection**.
- Signs should be prominently displayed on the ATM and within the premises to the effect that there are no keys available on the premises to allow access to the contents of the ATM.
- 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. The insurer will be able to assist.
- A security collar (of the type associated with gaming machines) or an anti-lasso device, should be fitted where removal of the ATM is a risk. This will be the case where the ATM could be readily extracted from the premises using chains and a powerful vehicle, even in the presence of obstacles such as partition walls. Where such devices are deployed, these should be attached to the main body of the ATM itself and not to the exterior facings.

To provide a deterrent to theft of or from the ATM, one of the following options should be installed:

- a security fog device conforming to BS EN 50131-8: 2009 **Alarm systems. Intrusion and hold-up systems. Security fog device/systems**, which should be designed to activate immediately if 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 device should protect, or be activated by, suitable alarm detection within any vulnerable roof voids;
- a banknote degradation system, which, when activated, dyes/stains/degrades currency notes in order to render them unattractive to thieves. This should be fitted to each ATM cassette contained in the ATM which holds currency notes.

  The banknote degradation system should be designed to activate immediately if the ATM is moved or attacked by any means. If required, the system may incorporate a unique taggant (forensic coding system), although such systems should not be used in isolation. Where a security fog device or 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.

Important: For CIT Fill ATMs containing cash at all times, it is strongly advised that the recommendations regarding siting and fixing of the ATM, and the installation of a security fog device or a banknote degradation system are adopted, since these measures, in combination, provide the best deterrent to theft of the ATM or its contents.

Other security measures which may be implemented for CIT Fill ATMs include:

- fitting a tracking system to the ATM; and
- installing a closed-circuit television (CCTV) system, with or without a detection facility, to view the ATM (but not the ATM keypad). In addition to local viewing and recording, the CCTV system should ideally conform to BS 8418: 2010: **Installation and remote monitoring of detector-activated CCTV systems. Code of practice** incorporating a link to a remote video response centre (RVRC) outside trading hours.

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

Electronic copies may be obtained from www.riscauthority.co.uk.

RISCAuthority

administered by FPA Fire Protection Association