Cash-in-transit

Recommendations

Berne August 2024

Table of contents Page

Table of contents (cont.) Page

1 Introduction

The initial cash-in-transit document was developed by the UPU Postal Security Action Group's Cash-in-Transit Subgroup in October 1998 and published as UPU security document No. 13. This historical document was reviewed for content and relevance by a team of subject matter experts (SMEs) under the Postal Security Group, who deemed it to be largely fit for purpose with small updates to reflect the current technological advances in the world.

The purpose of the cash-in-transit document continues to be to suggest ideas for an operational model to be used to enhance the security of transport within the postal supply chain.

The recommendations are based on the combined knowledge of the previous subgroup members and current SMEs of existing procedures and technical equipment used to secure cash-in-transit.

This paper does not include recommendations on paper procedures for cash-in-transit: such procedures can be decided upon locally without affecting the value of the recommendations.

This document contains only proposals for preventative measures to ensure greater safety of staff, equipment and cash at risk from attacks, as well as proposals for precautions during and after an attack.

As the past and current document has been prepared by a member group representing a relatively restricted number of countries, one or more countries may have implemented fully operational security equipment and procedures which are not known to the group members.

The document should be viewed only as a guide open to adaptation according to local geographical, political and economic considerations.

Reliability of delivery and service are, of course, essential factors that must be part of the considerations as well.

The crime rate in the individual country is a major factor in the planning of preventative measures to ensure a greater degree of safety.

Given the significant technological and electronic progress in the field of security equipment as elsewhere, the recommendations in this paper may very quickly be outrun by new products.

The document should generally be considered an index of ideas for security equipment and procedures to be implemented in order to enhance the security of transport.

However, it is strongly recommended to make sure that initiatives to enhance security are based on thorough risk assessments of local crime patterns and conditions for cash transport.

Proposals and/or ideas for improving the present paper's use value are most welcome and should be sent in English to the UPU Security Programme Manager at security@upu.int.

Recommendations

2 Cash centre

The security measures outlined in this chapter are considered best practices and are subject to how much control the reader of this manual has over the physical layout of a property, as well as the controls within it. These recommendations take this potential limitation into account. For example, the cash handling centre may be part of a major building complex whose perimeter and shell protection depends on the use of the building and the other entities which constructed it and use it, or the other functions that occur within that building. There may also be instances, in more densely populated areas, where these types of perimeters are not possible. In these instances, where the control of those security measures listed in this chapter is outside the purview of the reader, it may be necessary to liaise with external entities and stakeholders, or come up with a suitable solution to mitigate risk.

Perimeter protection

Ideally, the building should be surrounded by a protective fence which should be at least three metres high and provided on the outside with anti-ram protection.

The fence should be:

– cramped in concrete to prevent undermining;

– topped by barbed wire;

– alarm-secured against cutting;

– under CCTV surveillance with movement detection (used with AI component).

The whole area between the perimeter protection and the building itself should be well lit day and night, e.g., by means of a photo electric cell. The area should be kept under CCTV surveillance. (The use of LED lighting should be considered.)

Staff should be given access via electronic access control, possibly combined with visual control. Access to and from the centre should be given via turnstiles letting only one person at a time go through the entrance. If turnstile access is linked to the access control system, “anti pass back” or another preventative measure should be instituted. Ideal access control will incorporate the use of biometrics.

For practical reasons, separate turnstiles might be used for persons going into and out of the centre.

Vehicles should be given access to the centre through fence gates – one for vehicles moving into the centre and one for vehicles moving out of the centre. The external gate of the perimeter security system might be activated via a signal from the vehicle, while an electronic access card might be used for activating the internal gate under surveillance by a control centre or under visual control.

The perimeter gate system should either be provided with automatic anti-ram protection, or the gates should be resistant to “crashing”.

Vehicles used for maintenance service calls should be given access to the centre via the control centre on a case-by-case basis.

Depending on the circumstances, such maintenance vehicles should be checked when granted access to the centre. For instance, it may be relevant to check the undercarriage for smuggling of persons or other items.

Access from the cash centre should be given via a signal from the vehicle or activation from the control centre.

It should be possible to block all access roads from the control centre of the building.

Parking within the perimeter protection area should be restricted to postal vehicles used for cash-in-transit to and from the centre.

Building

The best solution is an independent building of a solid masonry or a concrete construction which is sufficiently secured to resist burglary and other forms of intrusion.

Windows

Only administrative and collective premises, e.g., cafeterias and breakrooms, should be provided with windows.

If required, production facilities might be equipped with roof lights.

As a minimum, all windows should comply with the current international security standards.

Windows should be:

– mounted as fixed windows which cannot be opened;

– mounted in such a way that they cannot be removed from the outside;

– provided with alarms indicating attempted breaking of the window.

Emergency exit doors

Emergency exit doors should be limited to the number required by law and for the safety of staff. It should not be possible to open emergency exit doors from the outside without the use of a key. Emergency exit doors should not lead to an area with public access, but ideally to an area within the perimeter protection via a secure airlock system (or in the case of one within a building complex, the emergency exit doors should ideally lead to an area within the complex but *NOT* to an area of public access).

Emergency exit doors from the cash handling area should in any case lead to an area within the shell protection.

Emergency exit doors should be provided with audible alarm systems for when the doors are opened, and kept under CCTV surveillance, ideally from both inside and outside.

Evacuation

In the event of an evacuation because of fire, threats, etc., valuables should, in principle, be secured as they would be outside normal working hours, i.e., placed in safes.

This should of course not be done to the detriment of staff safety. Therefore, the control centre should be notified without delay of any evacuation in order for the necessary precautions to be taken. A complete continuity-of-operations plan to include disaster risk management should be in place to include the cash centre. Further guidance may be found on the UPU website.

Access roads

Access roads to the building should be limited to the greatest possible extent.

Staff should be given access to the building via turnstiles and by the use of electronic access cards, possibly combined with visual entrance control or additional personal identification. From the first access road, access should be provided only to the collective facilities of the building.

Service people/suppliers who might be prevented from entering the building through turnstiles should be given access to the collective facilities via a separate, closed-access road.

Vehicles used for delivering and/or collecting cash should use a separate gate, see below.

All doors should be provided with audible alarm systems for when the doors are opened, and kept under CCTV surveillance. Doors used exclusively as emergency exits should be permanently secured by alarms.

Collective facilities

In principle, collective and administrative facilities should be open to all employees. Corridors should be secured by alarms outside normal working hours.

Cash handling area

External walls

The cash handling area should be constructed of materials that will resist burglary and other forms of intrusion. This is imperative if the cash handling centre is part of a major building complex.

Walls should include intrusion detection systems to detect force or penetration.

Facilities

Facilities should be sufficient to keep staff from leaving the secured area during the working day. Canteens and rest rooms should therefore be located inside the secured area, but wardrobe or locker facilities outside the secured area. Outdoor items – bags and the like – should be prohibited inside the working area, and staff should be instructed to leave their personal belongings in the assigned areas.

From the working area there should be direct access to the wardrobe or locker facilities.

The premises should be kept under CCTV surveillance and be provided with hold-up and room alarms.

The premises should not be provided with windows. Where daylight is required by law, the premises should be provided with high windows and/or roof lights.

The windows should be:

– of a sufficient standard to resist breakage and as a minimum comply with current international industry standards;

– equipped with alarms indicating (attempted) attacks or window breakage.

In cases where the cash handling centre may be part of a major building complex, the following additional measures should be implemented for windows:

– mounted as fixed windows which cannot be opened;

– mounted in such a way that they or parts thereof (glass) cannot be removed from the outside.

Access roads

There should be only two access roads: one for vehicles and one for staff with direct work relations to the area.

Both access roads should be constructed as a secure airlock system. In situations where the cash handling centre is part of a major building complex, an additional security measure of electronic access cards in combination with a personal code should also be implemented.

Secure airlock for vehicles

It should be confirmed that vehicles/persons are authorized to pass the external gate (to the open area within the perimeter protection) before the gate is activated from the control centre.

The secure airlock for vehicles should be without windows and of the same standard in terms of security as the external shell of the building. Where this is technically impossible, the secure airlock should be provided with internal lattice protection or similar composition to optimize its resistance, especially outside normal working hours. Where it is part of a major building complex, the windows should be sufficiently secured to resist burglary or other forms of intrusion.

The secure airlock should be provided with an alarm, which as a minimum should be operative outside normal working hours.

The inner part of the secure airlock, including the part leading to the cash handling area, should be without windows and of the same standard in terms of security as the external shell of the building.

Where the secure airlock is used by non-postal vehicles, e.g., customers visiting the cash handling centre, discretion should be required from centre staff in order to avoid disclosing information about customers/ vehicles using the centre and the amount of cash-in-transit to and from the centre.

The secure airlock should be equipped with a motion detection system and a hold-up alarm. In addition, it should be kept under CCTV surveillance both inside and outside.

Handovers from the secure airlock to the cash handling area should be made via a bulletproof parcel gate or similar arrangement that prevents persons from entering the cash handling area from the secure airlock.

The parcel gate should comply with the security standard mentioned under “windows”.

The two hatches of the parcel gate should be equipped with alarms, which as a minimum should be operative outside normal working hours.

From the secure airlock, or from any vantage point, it should not be possible to look into the cash handling area.

From the secure airlock there should be direct access to separate rest rooms reserved for drivers/assistants. The entrance to the rest room should be activated by the control centre or the centre employee servicing the vehicle in question.

The person letting a user go through the entrance to the rest room is accountable for that person. In other words, they should check that the user in question, including their vehicle, is led out of the building again via the secure airlock for vehicles.

The rest room wall facing the cash handling area should be of the same standard in terms of security as the external shell of the building.

Secure airlock for persons

Access should be given via a passage closed off by gates that only let one person at a time go through the entrance or via turnstiles, possibly combined with weight control or some other kind of personal identification. The secure airlock should not be provided with windows. The secure airlock and gates should be of the same standard in terms of security as the shell of the cash handling area.

The secure airlock should contain the following controls:

– Hold-up alarm;

– Motion detection system;

– Door alarms which indicate unauthorized access or opening outside normal working hours;

– CCTV surveillance both inside and outside.

Vaults

The location of vaults should take account of daily working routines and safety considerations.

All six sides of the vault should be of the same standard in terms of security. The walls should not adjoin outer walls. If located in the shell area, the vault should be surrounded by an observation corridor measuring a maximum of 50 cm in width. The door and door frame should at least be of the same standard in terms of security as the vault itself.

The door of the vault should be provided with:

– at least two non-interdependent locking devices;

– a burglar alarm covering at least one locking device;

– a timer that prevents unlocking outside fixed hours;

– a device preventing the door from being locked when somebody is inside the vault;

– a device on the inside of the door enabling emergency exit in the event of confinement or failure/ sabotage of the above security equipment.

Electric light in the vault should be switched off automatically if nobody is in the vault.

If the vault is equipped with a ventilation system, pipes should be protected against permeation or against “injection” of gasses and the like.

If the door of the vault is open during normal working hours, the entrance should be blocked by a lattice gate through which only authorized staff can pass, e.g., by means of electronic access control.

The vault should not be used for items that do not necessarily have to be kept in a safe.

The vault should be equipped with:

– alarms in the walls, floor and ceiling;

– a space disturbance detector;

– a hold-up alarm.

If safes are used instead, these should be fixed as a structural part of the building (floor/wall).

Access control

Access to the cash handling area should only be given to persons with direct working relations to the area.

As a minimum requirement, access should be given by means of a card combined with a personal code and visual recognition.

The personal code should be generated automatically by a computerized system.

Access control should be based on the so-called anti-pass-back system, which means that a personal code with anti-pass-back needs to be used to pass through the outside and the inside gates and vice versa.

As an added measure, where the cash handling centre is part of a major building complex, service and maintenance personnel should be vetted in the secure airlock and have their information recorded in a visitors' book prior to being given special permission by authorized personnel to access the cash handling area.

To optimize safety, access to the cash handling area should be controlled by separate access control with hardware as well as software located on the spot.

Biometric readers (facial, eye, fingerprint recognition systems) are strongly recommended in such areas over access cards with PIN codes.

Alarm systems

The building should be equipped with two separate alarm systems, one covering the administrative functions, the other the cash handling area. In cases where the cash handling centre is part of a major building complex, the span of control (such as the external access road) may be controlled by a separate entity. In situations such as this, a solution should be worked out between all stakeholders for effective communication and protocols in the event that an alarm is triggered, whether by the external entity or the personnel within the cash handling area.

Hold-up alarms should be installed in all relevant areas, and as a minimum:

– at external access roads;

– in the secure airlock for vehicles to the cash handling area;

– in the secure airlock for persons to the cash handling area;

– in the cash handling area;

– in the vault;

– remote alarms carried by staff on their person at all times.

The alarm system should be installed within the alarm-protected area(s). When activated, all alarms should alert law enforcement directly. Relevant parts of the building should be equipped with signs warning people of the presence of alarms.

It is extremely important that relevant persons in the building be very familiar with the appropriate reactions to the different alarm types.

Optimal, highly secured transmission systems should be used for the transmission of alarms.

Hold-up alarms and other relevant alarms from the area outside the cash centre should also alert the cash centre itself, as they may indicate that a criminal activity is brewing.

In that case, valuables should be secured as stated under “Evacuation”.

Should the primary alarm system fail for any reason (tampering, power outage, etc.) a backup plan should be in place to perform the same function. This backup plan can take many forms, such as the usage of mobile phones or radios.

CCTV surveillance

Two separate CCTV systems are recommended. Span of control may be limited when the cash handling centre is part of a major building complex, but a CCTV system is imperative for the cash handling area.

One system should cover:

– the perimeter protection;

– the area between the perimeter protection and the outer shell;

– the outer shell;

– the external access roads;

– the collective areas.

The other should cover the cash handling area, including:

– the secure airlock for vehicles, inside as well as outside;

– the secure airlock for persons, inside as well as outside;

– the working area and the entrances to all adjoining premises;

– the vault itself and the entrance to the vault;

– emergency exit doors, inside as well as outside.

The CCTV system covering the cash handling area should be “under control” and located within the premises or, in the case of a major building complex, located in the cash handling area itself.

The recorded surveillance should be transmitted to the control centre outside the cash handling area and possibly also to local law enforcement. Transmission of the recorded surveillance could, for instance, be arranged to take place only when alarms in the cash handling area are activated.

Recordings from the previous 31 days should be stored as a minimum. This applies to both systems.

3 Destinations

3.1 Security level

To optimize the safety of drivers/assistants and other staff, security levels should be adapted to the technical equipment and capability of the individual transport means.

In this regard, secure airlock systems constitute an optimum security level, but other systems such as the so-called “vehicle to wall” handover also deserve consideration.

3.2 Internal security steps

Nothing is stronger than the weakest link in a chain. Criminals seek and find places of easy prey.

Efforts to establish adequate conditions of safety at cash centres and for transportation should not be undermined by inadequate protection where the transport handlers service places of collection and delivery.

Building and access conditions

– It should be ensured that unauthorized persons are not given access to the building/premises via unlocked doors and open windows.
– All internal doors with access from the counter premises should be locked to prevent criminals from hiding inside in preparation for an attack.
– No persons, including persons wearing a uniform, should be given access to the building/counter premises before or after normal opening hours. Service people, law enforcement, etc., should only be given access against identification. Picture identification should be an invariable requirement. To ensure that access is given to the right persons, checks of their identity may be supplemented with a phone call to their employer.

Valuables/handover

Valuables should be securely stored and not be removed from safe boxes and the like before the arrival of the security van.

Likewise, cash handed over from the security van should be stored under safe conditions.

It should not be possible for unauthorized persons to observe cash handovers of any kind, e.g., from counter premises or through windows from outside the building.

Safe boxes should to the greatest possible extent be located in the premises where the handover takes place.

During the handover, the premises should be locked and equipped with a hold-up alarm and a telephone.

During the entire stay, the transport handler should be accompanied by a colleague from the destination, i.e., from arrival of the security van outside the building until the security van has left the place.

3.3 Security procedures

It is important to have checked the security level of the individual destinations prior to the handling of cash, especially where the premises are not specifically intended for the handling of cash, etc.

As a minimum, security procedures should involve:

– access conditions;
– stopping places;
– access roads;
– cash handling areas;
– assistance/observation;
– training.

Appendix A illustrates an example of a form to be used in connection with security procedures.

The observance by external customers of established written security procedures should be an invariable requirement.

3.4 Reporting systems

Examples of surveillance and reporting systems are given in section 6.

It is important to notify the destination of the arrival of a security van and to keep the destination advised of any difficulties that may arise.

In this respect, one or more persons should be on guard outside the destination and report back to the destination if they notice anything suspicious.

If anything suspicious is noticed, the security van should be warned against driving to the destination.

Notification of arrival may take place in different ways, e.g., via:

– GPS;
– mobile phone call from the security van;
– information from the control centre;
– phone call from the previous destination on the route.

3.5 Cooperation

As mentioned in section 3.3, the destination should be guarded against possible attacks before the arrival of a security van.

Cooperation between the destination and the security van should also include assistance in:

– notifying the security van of anything suspicious observed;
– receiving the security van;
– accompanying the security van to and from the cash handling area;
– ensuring departure of the security van without problems.

Local staff at the destination should be trained in:

– reactions during and after a robbery;
– alarm calls;
– observation;
– descriptions of robbers involved;
– psychological reactions of staff and customers.

4 Security vans

The pros and cons of a security van being of neutral appearance or not can be disputed.

Criminals are, as a general rule, presumed to prefer having clear signs indicating that the van is a security van.

However, a security van which is clearly marked as belonging to the Post will also raise the awareness of passers-by and thereby possibly attract more witnesses in the case of exposure to a crime.

It is of course very important that the crew of the van be familiar with the different security systems etc., of the van.

Any uncertainty with regard to routes and access conditions may affect relevant security measures to be observed by the crew.

Written instructions and relevant forms should be at hand in the security van.

Before departure, alarms and other security systems linked to the control centre should be checked.

Equipment required for road safety, such as head and rear lights, should also be checked to prevent “undue” stops by traffic control officials or local law enforcement and, in particular, to avoid the risk of being stopped by those impersonating local law enforcement.

4.1 Security level

The chosen security level should be commensurate with the amount of cash transferred as well as with local crime patterns.

The extensive use of armoured vans is now gradually being replaced by technical solutions, such as colour systems, to protect cash. For this reason, the tendency is towards armoured cabs only.

However, the said colour systems may be of no value depending on the packaging used for the cash-in-transit.

Likewise, customers may order transport of valuables that do not stand up to being secured by colour systems.

In such cases, the use of 100% armoured vehicles and/or vans sufficiently equipped to protect the valuables in question should be considered.

The security van or parts of the van should be bulletproof to protect its crew only.

Before adopting a bulletproof system, the chosen method should have been tested in accordance with, for example, the German industry standards (DIN) or similar security standards.

In Europe, most security vans are armoured according to security standards 2, 3 and 4.

The most commonly used method is to provide security vans with “armoured steel” and/or ballistic security. Ballistic security has the advantage of being made of a material that is considerably lighter than steel.

The windows of a security van should, at the very least, be protected to the same security standards as the armoured parts of the van.

It should be emphasized that “bulletproof” protection is not necessarily the same as “resistance to burglary”. Where a security van is provided with ballistic security, any noticeable resistance to burglary should therefore not be expected, apart from that provided by the original shell of the van.

4.2 Security equipment

Access to the security van should be given via a secure airlock function. Immediate, unimpeded access to the front and back doors of the van should be possible only when the van is parked in optimally secured areas, e.g., in the secure airlock system of the cash handling centre.

The front and back doors should be secured against normal breaking, i.e., the door lock should be considerably reinforced.

Access to the secure airlock may be given in different ways, e.g., via:

– activation from the cab;
– ordinary key (not recommended);
– electronic access control possibly combined with a PIN code;
– finger/hand identification (Biometrics);

possibly combined with:

– turnstiles;
– weight control.

In the event of a road accident, given that it should not be possible to open the doors of a security van from the outside, the van should be equipped with emergency exit doors.

Opening of emergency exit doors should only be possible from the inside of the van.

Where strongboxes/containers are secured by a smoke system, consider installing a separate air exhauster which will be activated automatically should a strongbox burst.

A security van should also be equipped with:

– a strong hand lamp;
– a fire extinguisher (powder);
– a first aid kit;
– relevant forms (description and observation forms – see also section 10);
– relevant phone numbers, instructions, etc.

4.3 Alarm equipment

To optimize the safety of drivers of security vans, the vans should be equipped with alarms linked to a control centre or to a security service – see also section 6.

Though they have a certain preventative character, alarms do not prevent attacks on security vans.

However, alarms may contribute to:

– determining the position of the security van;
– urgent calls for assistance;
– urgent action by law enforcement.

The following should be secured by burglar alarms:

– the two front doors;
– back doors;
– emergency exit doors;
– the engine bonnet;
– the fuel tank cap;
– the secure airlock (against unauthorized opening).

A hold-up alarm should be installed in:

– the cab (both sides);
– the secure airlock;
– the store room.

In addition, the driver/other crew should be equipped with a portable hold-up alarm when leaving the security van on duty.

Whether and to what extent there should be fuel cut-out when a burglar or a hold-up alarm is activated should be considered.

See also section 6.

4.4 Video surveillance

Security equipment in the form of video surveillance is becoming more and more widespread.

Cameras should be installed in the exterior mirrors as well as in the secure airlock and in the store room. Recordings may be stored in the van or transmitted via mobile telephony to the control centre. The transmission of pictures may be restricted to take place only in the event of alarm calls from the security van (activation of hold-up alarm).

4.5 Tracing and/or guided route management

Thanks to GPS surveillance via satellites as well as AirTags and similar technology, it is now possible to determine/trace the position of a security van anywhere in the world.

In addition to enhancing the safety of cash transport, tracing is a practical route management tool.

In the event of alarm calls from a security van, it is possible for the control centre/security service to determine the exact position of the van and to follow the van. This gives law enforcement/rescue teams better opportunities to target their actions.

Through guided route management, alarms are activated in the event of internal or external attempts to "remove" the security van from a guided route programmed in advance.

Antennae used for tracing and/or guided route management (especially GPS) are vulnerable to attacks and should therefore not be visible.

See also section 6.

4.6 Roof markings

To facilitate investigations by law enforcement, it is recommended to provide security vans with roof markings.

Roof markings may consist of a combination of letters and figures.

To enable law enforcement to see them both from the air and from the road, markings should:

– be mounted on the roof and measure e.g., 50 x 7 cm;

– be mounted on the front and at the rear of the security van.

The layout of roof markings and the choice of letter/figure combinations should be decided in cooperation with law enforcement.

5 Transport equipment

5.1 Integrated systems

As mentioned earlier, the extensive use of bulletproof security vans is now gradually being replaced by electronic security systems, the core of which is programming of containers/strongboxes via computerized solutions. These systems are often used in combination with colour smoke systems intended to make cash less attractive as a robbery object because of the risk of it being rendered useless.

Technological progress in this field is rapid and extensive.

Containers/strongboxes are opened by an electronic key (a so-called Dallas Key).

Any attempts to open the container/strongbox other than by an electronic key will release smoke and/or colour. Where the container/strongbox is protected by an alarm system, this will be activated.

Some systems require special equipment (e.g., racks) in the security vans, whereas others do not require any particular installation.

In addition, to diminish risks, electronic systems are used to secure cash during the whole process from counting it at the post office to handling it in the cash handling centre.

All systems have certain advantages and certain disadvantages.

The choice of system should depend on the individual user's standard-level requirements.

5.2 Strongboxes/containers

Given the many different types and sizes of strongboxes/containers, it is up to the users to decide individual requirements.

Some types require special equipment (e.g., racks) in the security vans, whereas others do not require any particular installation.

Security vans equipped with a smoke system should be provided with a separate air exhauster which should be activated automatically via a smoke detector.

Common to strongboxes/containers is the fact that the market is swamped with products, some of whose quality in terms of security is probably questionable.

Testing of the products by a neutral testing body is therefore strongly recommended.

Tests should include:

– a technical test;

– an environmental test;

– a crime technical test.

It is also important to test the adopted colour system for dyeing percentages and for colour resistance.

The following standards (from the Swedish standard) are recommended for dyeing:

– 95% of the banknotes should be dyed on at least 30% of their surface;

– two of the individual banknote’s edges should be dyed by at least 30%.

Both inking and dyeing by smoke are offered on the market.

Recent studies have shown that inking provides the best results. Where chemicals are added to the ink, it is moreover possible to attribute the inking in question to a specified user.

The advantage of smoke is its alarming nature and the fact that it can easily be seen when released.

A combination of the two systems may advantageously be used in some cases.

How the banknotes are packed is another decisive factor in efficient dyeing.

For the sake of the safety of people involved, it is important that the chemicals used have been approved as causing no injury to persons.

People involved in using the equipment should be instructed in:

– precautions against unintended breaking;

– actions to take in the event of breaking, including measures on how to protect persons.

5.3 Tracing/alarm systems

Regardless of the choice of equipment, it is possible to combine the equipment with tracing and/or alarm systems.

Alarm systems may sound at the site of the crime (audible alarm systems) and/or directly contact a control centre.

Alarms may also be activated from the opposite direction in the event of release of smoke or colour from the control centre.

Tracing takes place via the control centre.

Alarms are activated via the existing communications network.

Tracing may take place via GPS, using AirTag or similar technology surveillance, via satellites in combination with the existing communications network.

GPS antennae in strongboxes/containers are very vulnerable and can easily become inoperative.

It is also possible to set up your own position-finding antennae in combination with your own communications network.

Position-finding antennae are rather expensive and are mostly found in larger towns only.

The latest development is position finding via the existing GSM mobile telephone network. This is less vulnerable than tracing via GPS. The great advantage of this concept is that it works in places where an ordinary GSM mobile telephone functions and consequently does not require the setting up of “new” equipment.

See also section 6.

6 Surveillance

6.1 Security level

Surveillance of cash transport is an absolute prerequisite for preventative actions against attacks.

Surveillance may take a very simple form, using ordinary telecommunications combined with manual registration of reporting times as well as paper-based maps and route indexes.

However, the trend is towards advanced computerized systems: GPS surveillance, AirTags and the like.

Surveillance systems cannot prevent attacks, but they can reduce the risk of attacks.

6.2 Control centre

The control centre keeps security vans under surveillance.

Security vans may be kept under surveillance by a local control centre, or surveillance may take place by means of advanced, centrally located equipment.

Surveillance may also be performed by an external security service (outsourcing).

The security level of a local control centre should be in line with the recommendations in section 2 as regards:

– perimeter protection;
– shell protection;
– windows;
– emergency exit doors;
– access roads;
– secure airlock for persons;
– access control;
– relevant elements of alarm and CCTV surveillance.

6.3 Simple surveillance

The simplest method is via ordinary telecommunications.

Simple surveillance may take place between:

A. security van and branch office;

B. security van and control centre;

C. branch office and branch office;

D. branch office and control centre.

A. Security van and branch office

Via mobile telephone, the van keeps the branch office advised and notifies the office of the arrival of the van. See also section 3.3.

In the event of disruptions to this procedure, the branch office will react, i.e., inform the head office of the situation or call law enforcement.

B. Security van and control centre

Via mobile telephone or other communications equipment, the van notifies the control centre of the arrival at and/or departure from branch offices.

Where the distance between the branch offices is fairly long, position updates are advisable.

In the event of disruptions to this procedure, the control centre will react as in A.

As an extra security measure, the control centre may notify the next branch office on the route of the expected arrival of the security van at that office. See also section 3.3.

C. Branch office and branch office

The next branch office on the route is notified of the expected arrival of the security van via an ordinary phone call from the previous destination.

In the event of disruptions to this procedure, the “next branch office” will react as in A.

D. Branch office and control centre

When the security van leaves the branch office, the control centre will receive an ordinary phone call from that office to check that everything is OK.

In the event of disruptions to this procedure, the control centre will react as in A.

As an extra security measure, the control centre may notify the next branch office on the route of the expected arrival of the security van at that office. See also section 3.3.

If the security van does not arrive as expected, the “next branch office” will react as in A.

Position messages

To enhance the safety of drivers on “long-distance” routes, position updates (e.g., every half hour) are advisable.

6.4 Advanced surveillance

A very extensive range of equipment of varying levels of sophistication is offered by a host of different suppliers.

This document deals only with the most commonly used systems.

In principle, all these systems are operated either by their own control centre or by an external security service (outsourcing).

A short presentation of the following systems is given below:

– transmission systems;
– burglar alarms;
– hold-up alarms;
– GPS/AirTag, etc.;
– other tracing systems;
– guided route management.

Transmission systems

The best method is to use an ordinary mobile telephone to establish quick contact with a control centre or law enforcement. Use short code dialling.

Mobile telephony may also be used as a fixed installation linked to the various pieces of security equipment in the security van – see below under “alarms”.

Mobile telephony has the great advantage of worldwide coverage, though an overloaded network may sometimes delay linking.

Radio telephony on your own established radio network may therefore be a safer method. However, it is rather expensive to establish, especially where wide coverage is required.

In short

It is advisable to use your own radio network where local coverage is required and the density of security vans is high.

It is advisable to use mobile telephony where wider coverage is required and the density of security vans is low.

Burglar alarms

As mentioned under section 4.3, high-risk “zones” of security vans should be equipped with burglar alarms enabling the control centre to:

– reveal burglars hiding in the security van;
– call for assistance;
– stop the security van if in the hands of burglars.

Hold-up alarms

Security vans and drivers/other crew should be equipped with hold-up alarms enabling the control centre to:

– call for assistance if somebody is injured;
– ensure that law enforcement is quickly called out;
– stop the security van if in the hands of robbers.

GPS

By means of surveillance via satellites, it is possible to determine the position of a security van to within a few metres.

Via signal transmission from a number of satellites (normally 3–6), GPS equipment installed in the security van communicates the position of the van to a control centre enabling the control centre to notify law enforcement of the exact position and movement of the van.

Signal transmission from the security van to the control centre may take place via your own radio network or via mobile telephony.

GPS surveillance via satellites is a good and fairly inexpensive security measure. (Use AirTags or similar technology).

However, GPS antennae are vulnerable to any kind of covering; they should not be visible.

As the GPS antenna needs to point towards the sky, GPS surveillance is not suitable for tracing (stolen) objects such as containers/strongboxes.

Other tracing systems

A separate network of position-finding antennae has proved an efficient method for the tracing of objects.

Placed in the object (strongbox/container), the transmitter is released either manually or automatically.

Via the position finding antennae, signals are transmitted to a centrally placed receiver which communicates positions via a software module.

Vehicles and/or helicopters are fitted with scanning equipment to be used for exact position tracing.

Given that the size of the equipment allows it to be hidden in banknote bundles, this system is often used to trace cash from bank robberies.

Guided route management

Guided route management – normally via GPS – can advantageously be used on routes where it is important that the security van does not deviate from its route.

Guided route management can be used to reduce the risk of external as well as internal criminal attacks against the security van.

To prevent unintended false alarms, a margin of deviation of perhaps 100 metres from the route should be allowed.

Mobile telephony

Where tracing is carried out via the existing mobile telephone network, the “switched on” mobile phone is used to inform the control centre of a given position.

In order to prevent a serious drain on its battery, the mobile phone may be “switched on” via a call to an integrated “public pager” having a battery capacity of e.g., one year. When receiving a call, the pager will automatically switch on the mobile phone.

The control centre should therefore have the necessary software to show the position of the antenna and its “coverage area”. In urban areas, the position of a given object can be established within a 500 metre radius; in other areas within a larger radius.

For exact position tracing, a special transmitting unit is required. In addition, vehicles and/or helicopters with special scanning equipment will have to be used for exact position tracing.

Tracing via mobile telephony has the advantage of the existing mobile telephone network being used.

However, tracing via mobile telephony is not at present suitable for the tracing of cash from bank robberies.

Power supply

In addition to transmitting capacity (antenna), power supply is a prerequisite for the tracing of objects and should therefore also be considered in connection with the choice of system.

7 Route planning

The two main purposes of route planning are to ensure that:

– the routes are planned in a way that reduces the risk of attacks;

– urgent assistance is provided in the event of an attack.

Measures to prevent attacks

In planning routes, three main principles should be taken into account, namely:

– safe routes;

– varying times;

– varying routes.

The chosen roads should have traffic levels such that it is difficult for criminals to hide before a planned attack and in order to have witnesses during and after an attack.

Roads with few access and exit points make it difficult for criminals to escape and easier for law enforcement to bar. In this regard, motorways constitute safe routes.

The transportation of cash may also be arranged by means of guided route management.

Monitored by GPS satellite surveillance (using AirTags or similar technology), the security van will follow a guided route programmed in advance. Should the security van deviate from its route, an alarm will be activated which will alert the control centre.

Varying times helps to confound criminals and spoil attack plans.

Driving in daylight is recommended as darkness makes it easier for criminals to prepare their action and to slip away unobserved afterwards.

Varying routes helps to sharpen drivers' attention, and reduce the tedium of daily routines. Also, varying routes discourage drivers from taking an active part in a crime and thus help to prevent them from coming under suspicion of involvement in it.

8 Cash and other valuables

8.1 Packing and packaging

The purpose of packing and packaging is to protect cash against internal as well as external crime, i.e., unauthorized seizure of the individual banknotes. In principle, the driver and other crew should not know the amount of cash transported.

Different types of seal may be used, such as wax or lead seal, tape, etc., and the range of sealing products offered on the market is extensive. However, it is recommended to use sealing products with substantiated protective properties.

The type of packaging used should make allowance for the efficiency of any colour or smoke systems.

8.2 Receipt

The issuing of receipts is advisable on account of:

– internal security requirements;

– customers;

– insurance companies.

In principle, the persons who legally receive cash and other valuables are liable for the cash and other valuables in question, though receipts should solely be given for the number of sealed lots received and not for the amount of cash contained in them. Where, in rare cases, receipts are given for an exact amount, the recipient should check the amount.

To avoid any kind of suspicion, the person who has given a receipt for cash to be reforwarded to another destination should obtain a receipt for the cash when passed on to the next destination. Receipt procedures may differ according to the practical transport arrangements.

Receipts may be issued on paper or electronically.

The issue of receipts is important to customers and insurance companies, given the need to establish the liability for cash and other valuables at critical times, i.e., in connection with handover procedures or in the event of a robbery.

Adequate receipt procedures should therefore be used as evidence of the cash transport company being a reliable and security-minded cooperation partner.

Where several insurance companies are involved in a “transport chain”, it is important to ensure that the time when the liability is transferred from a legal entity to another cannot be disputed.

Also, it is important to ensure that the amount of cash transported never exceeds the amount for which full coverage would be given by insurance companies in the event of a successful attack.

Finally, it should be ensured that other procedures and technical equipment comply with the insurance terms.

9 Staff

9.1 Daily travel

The number of staff involved in the transport of cash depends on local conditions, including local and/or national crime patterns.

Other decisive factors are:

– the equipment of the security van;

– technical equipment;

– the amount of cash involved;

– legal conditions;

– agreements with trade unions and staff organizations.

It should be emphasized that a decisive factor in terms of security is not the number of responsible staff, but the conditions and security equipment in place for ensuring optimum safety.

Staff should not work the same routes for several days in succession. In addition, they should not know which route they are given until the start of the working day in question.

If the security van is crewed by a team of two or more members, an ongoing random replacement of team members should take place to prevent the same people from driving together all the time.

Regardless of the frequency of shifts (on a daily basis or otherwise), they should be randomly scheduled.

9.2 Personal security equipment

Depending on local conditions, including local legislation and crime patterns, the following security equipment is recommended:

– weapon;
– visor;
– bulletproof waistcoat;
– remote alarm;
– mobile telephone.

At the very least, personal security equipment should include a mobile telephone.

9.3 Recruitment

It is obvious that responsible staff should have a clean criminal record. A careful security check should therefore be made on these staff before recruitment. In addition, the security check should be followed up on a regular basis, e.g., every second year.

It should be ensured that the financial circumstances of a person and/or dependency on criminal elements do not involve the risk that the person in question is “forced” to abuse his or her position.

The need for staff to observe rules of secrecy should be emphasized. Accordingly, staff should confirm the observance of secrecy in writing.

In connection with the recruitment of staff, it is recommended to carry out the following tests, to be followed up e.g., every second year:

– a drug test;
– a test of reactions to psychological stress;
– an alcohol test.

It should be emphasized that the above tests are as much in the interest of the tested person (in terms of personal safety) as of the employer.

Close family relations to persons employed within the cash transport chain may also constitute a risk in terms of safety.

It should be checked annually that drivers have a valid and appropriate driving licence.

9.4 Training

An important safety aspect is that persons working in the cash-in-transit sector are given relevant training in the form of basic training and refresher courses (e.g., every second year).

In addition, ad hoc courses are recommended in connection with changed crime patterns etc.

The following are possible training subjects:

Basic training

– procedures and practices for cash transport and handling;
– security regulations;
– security equipment in security vans;
– types of security vans;

- communications equipment;
- alarm systems;
- use of personal security equipment and target practice;
- driving techniques – theory and practice (evasive actions);
- observation techniques – theory and practice;
- robbery exercises – theory and practice;
- prevention of crimes, i.e., theft, robbery, hostage taking, kidnapping;
- precautions during a crime;
- precautions after a crime;
- description exercises – theory and practice;
- psychological reactions;
- counselling after exposure to crime;
- review of relevant sections of national laws:
  - civil arrest;
  - necessity;
  - self-defence;
  - self-help;
  - trial;
  - duty to give evidence;
- cooperation with law enforcement;
- cooperation with the media and rules for statements to the media;
- first aid in connection with road accidents;
- firefighting – theory and practice.

Refresher courses

- driving techniques, particularly evasive actions;
- observation techniques – theory and practice;
- robbery exercises – theory and practice;
- description exercises – theory and practice;
- prevention of crimes;
- precautions during a crime;
- precautions after a crime;
- first aid in connection with road accidents.

10 Cooperation with law enforcement

10.1 Ongoing cooperation

Ongoing cooperation with law enforcement is important both for crime prevention and in relation to criminal investigations.

The purpose of ongoing cooperation with law enforcement is to familiarize them with transport of cash procedures so that they are fully equipped to deal with crimes against security vans, etc.

Input from law enforcement is also part of this cooperation.

Such input is useful in:

– implementing preventative actions;

– helping law enforcement investigate crimes.

As a minimum requirement, law enforcement should have general knowledge about transport of cash procedures, i.e.:

– routes;

– reporting systems;

– technical equipment of security vans;

– alarm systems;

– security instructions.

Likewise, drivers and other crew of security vans should have general knowledge about law enforcement work, i.e.:

– stop by law enforcement (by fake law enforcement);

– questioning principles;

– protection of evidence;

– investigation;

– hearing of witnesses.

To facilitate ongoing dialogue with law enforcement, the exchange of phone numbers and names of contact persons is recommended, as is an annual meeting between law enforcement and responsible staff.

To facilitate law enforcement work in connection with hostage taking and robberies, it may be useful for law enforcement to be in the possession of drawings showing the layout of premises, access roads, etc., of cash centres.

However, it is important to make sure that:

i the drawings are stored securely by law enforcement;

ii new drawings are made when a given cash centre is reorganized and a copy of the new drawing given to law enforcement;

iii old drawings are returned by law enforcement to avoid the risk of being employed by mistake in a given situation.

10.2 Exercises

To test the observations, reactions and behaviour of staff during and after a robbery, it is recommended to arrange regular exercises in cooperation with law enforcement.

Such exercises may advantageously be performed in or at cash centres to limit external involvement as far as possible.

10.3 Stop by law enforcement

It is important to know that criminals often pose as law enforcement before and during a planned attack.

Wearing a law enforcement badge and uniform does not always indicate that the person in question is a law enforcement officer.

To avoid undue stops by law enforcement, the following should be observed:

– road safety;

– road traffic laws;

– speed limits.

If stopped by law enforcement, it is extremely important that caution is observed by the driver of a security van.

Therefore, an agreement should be made with the local law enforcement on measures to take in the event that a security van is stopped by law enforcement, e.g.:

– disregard the instruction and drive to the next law enforcement station, notifying it of the stop;

– drive to the next law enforcement station;

– stop, stay in the van and contact law enforcement and/or control centre.

If a security van is stopped by fake law enforcement and actually stops, it is difficult to avoid attack.

10.4 Law enforcement escort

In many countries, security vans are under marked or unmarked law enforcement escort. Where protected by an escort, the security van may either be “crewed” by law enforcement or followed by a law enforcement car.

Law enforcement escort may be motivated by the need to handle:

– local crime patterns;

– considerable cash transfers.

Regular law enforcement escort may thus be part of the local law enforcement service or, as is most often the case, a service beyond normal law enforcement work.

In specific cases, however, it is common practice to enter into ad hoc agreements with law enforcement on law enforcement escort.

Where such ad hoc agreements cannot be reached with law enforcement, an alternative solution may be to ask a private security company for assistance or to use your own vehicles for escorting purposes.

In the event of an emergency (road accident and/or vehicle breakdown), protection by law enforcement escort should be a matter of course.

11 Road accidents and vehicle breakdowns

11.1 Road accidents

It is impossible to exclude the risk of road accidents.

However, it is possible to help reduce the risk of being involved in a road accident. This requires:

– a high degree of road safety;

– daily road safety checks;

– experienced drivers;

– driver training in driving techniques;

– drivers’ and other responsible staff’s awareness of their own responsibility.

It is important to distinguish between self-inflicted road accidents and road accidents in which a security van may be involved and which in no way appear to be staged.

11.2 Staged accidents

A common trick among criminals is to organize staged accidents in the hope that the security van that is the target for their attack will stop and come to their rescue.

In such cases, there is a need for extreme caution.

As a general rule, the driver should not stop but call for assistance via their mobile telephone.

The driver of a security van should also know that some criminals will stop at nothing (e.g., murder or mutilation) in order to reach their target.

In any case, drivers should never expose themselves and/or their colleagues to a dangerous confrontation with criminals who have chosen a security van as the object of an attack.

11.3 Self-inflicted accidents

In principle, assistance should always be given to people who are injured. In many countries, assistance is required by law as well.

Assistance may be provided in the form of:

– trying to stop the effects produced by an accident;
– calling a rescue team;
– providing first aid.

Assistance should of course be provided with extreme caution and in consideration of the amount of cash/kind of valuables transported.

The control centre should be notified of the accident and where a rescue team or others are ready to take care of the injured, the driver and assistant drivers should again concentrate on their own journey.

Wherever possible, the security van should never be left unmanned.

Guidelines should have been prepared in advance on measures to take in the event of a road accident involving car breakdowns so that urgent assistance can be provided by:

– a rescue team;
– law enforcement;
– postal units.

Where a security van is involved in an accident, transfer to another van should be carried out with the utmost discretion, preferably after the damaged security van has been removed, and if possible with the assistance of law enforcement who in any case should be notified of the situation.

11.4 Vehicle breakdowns

Where the security van stops because of engine trouble, a punctured tyre or other malfunction, no-one should leave the van.

Via mobile telephone, the control centre should be kept advised of the situation just as law enforcement should be notified of the breakdown so that the necessary assistance can be provided.

It should be emphasized, however, that breakdowns can, to a certain extent, be avoided by using vans of high quality and high standards of maintenance.

12 Measures to prevent robberies

In the previous sections we discussed a range of important crime prevention factors, such as adequate equipment and training.

However, other factors may contribute to crime prevention as well, e.g.:

– keeping “suspicious” persons under observation, possibly *in cooperation with* or with the help of law enforcement;

  (use of observation form below);

– advising colleagues or security guards at destinations of the arrival of security vans so that they can make observations in and around the destination;

– deviating from normal routines during transportation or on arrival at the slightest suspicion that a criminal attack is brewing.

Careful handling and common sense are thus basic crime prevention factors.

An observation form is provided as an example.

Observation form
Suspicious activity/person report form

***Purpose:** This form is used to document any suspicious activity or person observed within or around the premises. Employees should fill out this form immediately upon noticing suspicious behaviour to ensure accurate and timely reporting.*

Suspicious activity/person report

–

Section 1: Personal Information

– ***Employee name:*** _____

– ***Employee ID:*** _____

– ***Position/Title:*** _____

– ***Contact number:*** _____

Section 2: Incident details

– ***Date of observation:*** _____

– ***Time of observation:*** _____

– ***Location (specific area within/around the premises):*** _____

Section 3: Suspicious person description

1 ***Number of persons:*** _____

2 ***Gender(s):*** _____

3 ***Approximate age(s):*** _____

4 ***Height:*** _____

5 ***Weight:*** _____

6 ***Build (e.g., thin, medium, heavy):*** _____

7 ***Complexion:*** _____

8 ***Hair colour and style:*** _____

9 **Eye colour:** _____

10 **Distinguishing features (e.g., scars, tattoos, accents):** _____

Section 4: Clothing description

– **Headwear (e.g., hats, masks):** _____

– **Upper body clothing (e.g., jackets, shirts):** _____

– **Lower body clothing (e.g., trousers, skirts):** _____

– **Footwear:** _____

– **Accessories (e.g., gloves, bags):** _____

Section 5: Suspicious activity description

– **Describe the suspicious activity observed:** _____

– **What was the person doing?** _____

– **Was there any verbal communication? If so, describe:** _____

– **Describe the person's behaviour (e.g., nervous, aggressive):** _____

Section 6: Vehicle description (if applicable)

– **Vehicle make and model:** _____

– **Vehicle colour:** _____

– **Licence plate number:** _____

– **Other identifying features (e.g., decals, damage):** _____

– **Direction of travel:** _____

Section 7: Additional observations

– **Did the person interact with anyone else? If so, describe:** _____

– **Did the person enter/exit any specific area? If so, describe:** _____

– **Any other relevant details or observations:** _____

– **Security camera footage available? (Yes/No):** _____

Section 8: Witness information

– **Were there any witnesses? If so, provide details:**
  - **Witness name:** _____
  - **Contact information:** _____
  - **Relationship to employee (if any):** _____

Section 9: Reporting

– **Reported to supervisor (name):** _____

– **Date and time reported:** _____

Employee signature: _____

Date: _____

–

Instructions for completing the form:

*1 **Be observant:** Note down as many details as possible about the person and their activity.*

*2 **Be specific:** Provide clear and specific descriptions to aid in identification and investigation.*

*3 **Submit promptly:** Ensure the form is completed and submitted to your supervisor or the designated authority immediately after the observation.*

*4 **Stay safe:** Do not approach or confront the suspicious person. Maintain a safe distance and ensure your safety first.*

This form will help us maintain a secure environment and assist law enforcement if necessary. Your diligence in reporting suspicious activities is crucial. Thank you for your cooperation.

13 During a robbery

It is of course very difficult to know how someone will react to serious threats made by an armed criminal.

Where threats are made against drivers and other responsible staff, it is advisable to:

– keep calm;
– do as you are told by the criminal;
– presume that their weapon is genuine and that they will use it if forced to by the circumstances;
– not expose yourself or your colleagues to dangerous confrontations with the criminal;
– execute any orders steadily, but avoid provocation;
– try as far as possible to get into conversation with them – to determine their language;
– try to restrict the amount handed over, if possible;
– observe the criminal without staring at them;
– call for assistance when it is safe to do so.

14 After a robbery

14.1 Immediate actions

Very often there is complete chaos after a robbery and it may be difficult to remain calm in such a situation, especially where people are injured.

After a robbery, it is advisable to:

– keep calm;
– observe the escape routes of the criminal(s);
– call for assistance;
– contact law enforcement;
– provide first aid where people are injured;
– provide witnesses;
– protect any valuables that have not been stolen;
– seal off the place where the robbery has taken place to preserve evidence of the crime;
– notify the control centre of the robbery.

Hearings by and statements to law enforcement should be handled with the utmost discretion.

14.2 Description

Descriptions which are as accurate as possible are important to successful investigation by law enforcement.

To describe criminals easily and accurately, the use of description forms is recommended.

After a robbery, the form should be completed without delay by staff involved as well as by possible witnesses. Nobody should communicate details about the robbery before the form has been completed and relevant staff and witnesses have been heard by law enforcement.

An appropriate number of description forms should therefore be available in all security vans for distribution to possible witnesses in the event of a robbery.

The contents of the description forms may vary according to local conditions and should be determined in cooperation with law enforcement.

Description forms should contain the following information:

– gender, age, height;
– person type;
– body shape;
– race;
– language, dialect;
– face, hair, hair colour, beard, eye colour;
– hands, tattooing;
– weapon type;
– jewellery etc.;
– packaging of the proceeds (bags, etc.);
– dress;
– transport means;
– escape route;
– course of events.

To expect complete descriptions would of course be absurd. A few accurate details are preferable to a large number of “half-truths”, and this should be emphasized when training in description techniques is given.

Ongoing description exercises with subsequent comparison of replies is an important training tool which helps staff to deliver descriptions which are as accurate as possible.

An example of a description form is shown on the next page.

Description form
Description of robbery form

***Purpose:** This form is used to document the details of a robbery incident for training and reporting purposes. Employees should fill out this form as accurately and completely as possible immediately after the incident, while details are fresh in their minds.*

Robbery incident report

–

Section 1: Personal Information

- ***Employee name:*** _____
- ***Employee ID:*** _____
- ***Position/Title:*** _____
- ***Contact number:*** _____

Section 2: Incident details

- ***Date of incident:*** _____
- ***Time of incident:*** _____
- ***Location (specific area within cash centre):*** _____

Section 3: Robber description

1. ***Number of robbers:*** _____
2. ***Gender(s):*** _____
3. ***Approximate age(s):*** _____
4. ***Height:*** _____
5. ***Weight:*** _____
6. ***Build (e.g., thin, medium, heavy):*** _____
7. ***Complexion:*** _____
8. ***Hair colour and style:*** _____
9. ***Eye colour:*** _____
10. ***Distinguishing features (e.g., scars, tattoos, accents):*** _____

Section 4: Clothing description

- ***Headwear (e.g., hats, masks):*** _____
- ***Upper body clothing (e.g., jackets, shirts):*** _____
- ***Lower body clothing (e.g., trousers, skirts):*** _____
- ***Footwear:*** _____
- ***Accessories (e.g., gloves, bags):*** _____

Section 5: Weapon description

- ***Type of weapon(s) (e.g., gun, knife):*** _____
- ***Number of weapons:*** _____
- ***Description of weapon(s):*** _____
- ***Weapon colour:*** _____

Section 6: Robber's actions

– ***What did the robber(s) say?*** _____

– ***Describe their behaviour (e.g., calm, aggressive):*** _____

– ***Was anyone injured? If so, describe:*** _____

– ***What was taken (cash, valuables, etc.)?*** _____

– ***Estimated value of items taken:*** _____

Section 7: Getaway details

– ***Getaway vehicle (if any):*** _____

– ***Vehicle description (make, model, colour, licence plate):*** _____

– ***Direction of escape:*** _____

– ***Accomplices (if any):*** _____

Section 8: Witness information

– ***Were there any witnesses? If so, provide details:***

- ***Witness name:*** _____
- ***Contact information:*** _____
- ***Relationship to employee (if any):*** _____

Section 9: Additional information

– ***Any other details or observations:*** _____

– ***Security camera footage available? (Yes/No):*** _____

Section 10: Reporting

– ***Reported to supervisor (name):*** _____

– ***Date and time reported:*** _____

Employee signature: _____

Date: _____

–

Instructions for completing the form:

1 ***Stay calm:** Take a few deep breaths before filling out the form to ensure clarity of thought.*

2 ***Be accurate:** Provide as much detail as possible, even if it seems insignificant.*

3 ***Use descriptive language:** Use specific terms to describe the robbers and their actions.*

4 ***Submit promptly:** Return the completed form to your supervisor or the designated authority immediately after filling it out.*

This form will be used to help law enforcement in their investigation and to improve our security measures. Your cooperation and attention to detail are crucial. Thank you for your assistance.

14.3 The media

The media will often have entered the scene of a crime before law enforcement.

It is very important to ensure that any statements to the media do not prejudice law enforcement investigation or compromise security equipment, procedures, etc.

As a general rule, making statements to the media should therefore be a task reserved for law enforcement.

Media interviews with postal staff involved should first be cleared with the public relations manager of the postal company.

At such interviews, information about specific events should only be given by agreement with law enforcement. Details of the cash stolen should be given with caution. Moreover, details of cash amounts should never be revealed.

Concrete information about security systems and routines should never be given, whereas general references to crime prevention measures and adequate security systems are natural interview topics.

The media should be discouraged from taking photographs of the crime scene.

14.4 Reconstruction for broadcast media

Real-life crimes are a popular subject for many television programmes.

Such television programmes can also contribute to law enforcement investigation of unsolved crime cases.

As regards postal participation in crime reconstructions, it is advisable to bear in mind that:

– only the specific case should be highlighted;
– security equipment and procedures should not be disclosed, but crime prevention measures and adequate security systems may advantageously be mentioned in general terms;
– postal staff and/or witnesses involved in the specific case should not participate in the reconstruction;
– law enforcement should “lead” and approve the reconstruction;
– the reconstruction should be made in the presence of relevant postal management having the authority to intervene where required;
– before being broadcast, the reconstruction should have been approved by law enforcement and the postal company.

14.5 Contingency plan

A contingency plan should be prepared in which the individual responsibilities of people acting as helpers after, e.g., a serious road accident, robbery, hostage taking or kidnapping are clearly defined.

It is important that the contingency plan is implemented immediately after the event.

Helpers may, for example, be responsible for the following tasks:

– immediate help (psychological first aid);
– contact with a psychologist;
– contact with relatives;
– assistance and support in matters with law enforcement (review of photographs, identity parade, trial);
– practical tasks to be carried out immediately after the event;
– taking over of vehicle/new vehicle after the event;
– contact with law enforcement;

– contact with the media;
– in-house information about the event;
– provisional precautions to avoid the risk of additional damage or injury after the event.

15 Hostage taking and kidnapping

15.1 Security level

In addition to being exposed to a high risk in terms of safety, people who are taken hostage or kidnapped by criminals will suffer from a great sense of uncertainty as they are often held as prisoners by the criminals for a longer period.

The taking of hostages most often happens spontaneously when this is the only means for a criminal to escape during or immediately after a criminal activity.

Kidnapping is normally a planned action where the kidnappers – often after very thorough preparatory work – take one or more persons away by force in order to gain access to valuables or otherwise obtain valuables from persons or companies in exchange for returning their “prisoners”.

Both situations will usually involve heavy psychological trauma among the persons involved.

It is therefore important to have carefully considered the efforts required to deal with such events and to have internal contingency plans prepared accordingly.

In the case of hostage taking or kidnapping, law enforcement are expected not to take actions that will put people’s lives at risk.

Only people specially trained in negotiating with criminals (e.g., law enforcement) should initiate negotiations with them on ransom terms.

15.2 Hostage taking

As mentioned above, the taking of hostages most often happens spontaneously. Preventative measures are therefore difficult to implement in such a situation.

However, to diminish the risk of being taken hostage, it is recommended to try as quickly as possible to get beyond the reach of the criminals.

In the case of hostage taking, law enforcement should be notified of the situation without delay.

The hostage should be aware that, in principle, the criminal does not want to hurt them, but solely to use them as a means to escape.

To avoid running an undue risk, the hostage should:

– During the event:
  - keep a low profile;
  - keep calm;
  - follow given instructions;
  - avoid making jokes;
  - observe the criminal for later description (avoid staring at them);
  - not try to escape unless absolutely sure that escape is possible.
– After having been set free:
  - protect any traces of the criminals and/or their vehicle;

- contact law enforcement without delay;
- contact relatives and the place of employment;
- write down details of the criminals.

15.3 Kidnapping

Kidnapping is a more serious action which is not as frequent as hostage taking.

Kidnappers will normally demand a ransom of a considerable size to be paid to free a high-ranking person held as their prisoner.

Although high-ranking persons are the normal target of kidnappers, contingency plans should deal with measures to reduce the risk of any staff being exposed to a kidnap attempt.

To reduce the risk of kidnap attempts against security vans, it is advisable to observe “suspicious persons” as stated in section 12. In their preparations for kidnapping someone, kidnappers will often try to become familiar with the daily routines of their victim by following them at all times of the day. The observation by a potential victim or others of “suspicious persons” should therefore not be restricted to hours of duty.

A kidnapper will normally prefer to kidnap their victim without being observed by witnesses or others.

To avoid running an undue risk, the kidnapped person should:

– During the event:
  - keep a low profile;
  - keep calm;
  - follow given instructions;
  - avoid making jokes;
  - observe the criminal for later description (avoid staring at them);
  - not try to escape unless absolutely sure that escape is possible.
– After having been set free:
  - protect any traces of the criminals and/or their vehicle;
  - contact law enforcement without delay;
  - contact relatives and the place of employment;
  - write down details of the criminals.

Receipt of messages or calls from kidnappers

The person receiving a message or a call from kidnappers may play a decisive role in successful investigation of the crime by law enforcement.

Given the very useful information that may be disclosed during the conversation with a kidnapper, it is important that the person receiving the message or call:

– keeps calm;
– avoids interrupting the conversation;
– asks the same questions several times;
– observes noises and other voices;
– writes down as much as possible;
– completes the threat calls form (see next page).

Threat calls form

Phone call threat observation form

***Purpose:** This form is used to document the details of a threatening phone call received at the workplace. Employees should fill out this form immediately after the call to ensure that all details are accurately captured for reporting and investigation purposes.*

Phone call threat observation report

–

Section 1: Personal information

- ***Employee name:*** _____
- ***Employee ID:*** _____
- ***Position/Title:*** _____
- ***Contact number:*** _____

Section 2: Call details

- ***Date of call:*** _____
- ***Time of call:*** _____
- ***Duration of call:*** _____
- ***Phone number (if available):*** _____
- ***Call received on (phone extension/number):*** _____

Section 3: Caller description

1. ***Gender:*** _____
2. ***Approximate age (if discernible):*** _____
3. ***Accent or dialect:*** _____
4. ***Speech patterns (e.g., slow, fast, slurred):*** _____
5. ***Background noise (e.g., traffic, music, other voices):*** _____

Section 4: Threat description

- ***Exact words used (as close to verbatim as possible):*** _____
- ***Nature of the threat (e.g., bomb, physical harm, cyber threat):*** _____
- ***Specific details mentioned (e.g., location, time, demands):*** _____

Section 5: Caller's behaviour

- ***Tone of voice (e.g., calm, angry, nervous):*** _____
- ***Was the caller coherent or rambling?:*** _____
- ***Did the caller provide any personal information?:*** _____

Section 6: Call handling

– ***Questions asked to caller (if any):***

1 _____

2 _____

3 _____

– ***Caller's responses:*** _____

Section 7: Additional observations

– ***Any other relevant details or observations:*** _____

– ***Were any instructions given by the caller?:*** _____

Section 8: Action taken

– ***Immediate action taken (e.g., informed supervisor, called security):*** _____

– ***Name of supervisor Informed:*** _____

– ***Date and time supervisor informed:*** _____

Section 9: Reporting

– ***Reported to security/authorities (name):*** _____

– ***Date and time reported:*** _____

Employee signature: _____

Date: _____

–

Instructions for completing the form:

1 ***Stay calm:** Remain as calm as possible during and after the call.*

2 ***Be attentive:** Listen carefully and try to remember as many details as possible.*

3 ***Record immediately:** Complete this form immediately after the call to ensure details are fresh.*

4 ***Report promptly:** Submit the completed form to your supervisor or the designated authority without delay.*

5 ***Do not engage:** Do not provoke or engage aggressively with the caller. Follow safety protocols.*

This form is crucial for documenting and investigating phone threats. Your careful observation and prompt reporting can help ensure the safety and security of everyone in the workplace. Thank you for your attention and cooperation.

16 Psychological reactions and assistance

16.1 Psychological reactions

It is natural for psychological problems to follow from exposure to harmful situations, such as a robbery or a road accident. In medical terms, this is called "acute stress".

It is impossible to predict how different people will react to different situations.

Likewise, it is impossible to predict how the same person will react to different situations of the same character.

Also, some events may cause harm to persons who have not been directly involved in the harmful event.

As a general rule, persons who have been exposed to harmful situations need the assistance of colleagues as well as professional help.

It should be emphasized that professional help should be given as an offer for help, i.e., no person should feel constrained to receive it.

Professional help should be given no later than 24 hours after the event.

16.2 Psychological stress (phases) and assistance from colleagues

Reactions to psychological stress can be divided into four phases:

– shock phase;
– reaction phase;
– recovery phase;
– reorientation phase.

Shock phase

The shock phase is the period when a person suffers from shock, i.e., during and immediately after a harmful event.

A person suffering from shock may seem unaffected by the harmful event even though their mind is in a state of chaos.

A person may react actively to a shock by:

– crying;
– shouting;
– rushing around.

A person may react negatively to a shock by:

– staring blankly;
– hiding;
– fainting.

Colleagues may assist a person suffering from shock by:

– accepting their reactions;
– being supportive;
– providing relevant personal guidance;
– praising the person;
– contacting their relatives.

Reaction phase

The reaction phase is the period of the first couple of days after a harmful event.

The person is traumatized as the result of a harmful event.

The person may react to the trauma as follows:

– insomnia;
– tension;

– nightmares;
– being easily moved to tears;
– loss of appetite;
– tiredness;
– headaches;
– stomach pains;
– frayed temper;
– aloofness, isolation;
– lack of concentration, performance fluctuations.

Colleagues may assist the person by:
– accepting their reactions;
– listening to the person;
– letting the person tell them about the event without interfering or showing a we-know-better attitude;
– accepting repetitions;
– praising and never blaming the person;
– taking care that the person is never alone;
– avoiding jokes;
– offering alternative work, if desired.

Recovery phase

The recovery phase is the one-year period from the end of the reaction phase.

The person's well-being is gradually restored, and the person is able to perform their "old" duties without problems.

However, the person may have relapses if confronted with situations that remind them of the harmful event.

The person may react to relapses as follows:
– nervous fear;
– uneasiness;
– uncertainty.

Colleagues may assist the person by:
– accepting their reactions;
– letting the person talk about their "problems".

Reorientation phase

The reorientation phase is the period from the end of the recovery phase and forward.

The person is again in control of their situation though still remembering the pain caused by the harmful event.

16.3 Psychological first aid (assistance from colleagues) and professional help

In the shock phase as well as in the reaction phase, "psychological first aid" (assistance and support) from colleagues is extremely important.

Very often, there will also be a need for professional help, especially in the recovery phase and sometimes also in the reorientation phase. In-house assistance of this kind should therefore be available.

As a general rule, colleagues indirectly affected by a harmful situation should be offered professional help as well.

Assistance and support in external relations

The person(s) who have been exposed to a robbery, etc. will normally be requested to turn up at law enforcement for the purpose of:

– reviewing a collection of photographs;
– being confronted with suspects;
– giving evidence in trials.

However, the person(s) in question will often be reluctant to recognize the heavy psychological strains that follow from meetings of this kind.

In such situations, assistance and support will be required from colleagues according to the motto “you are not alone”.

16.4 Conclusion

Where a person has been exposed to a harmful event:

– a reaction will always follow in the wake of the event;
– reactions to the event are a natural thing;
– reactions to the event are not a sign of weakness;
– the person should accept assistance from colleagues as well as professional help.

Colleagues

– should be prepared for a harmful event;
– should be ready to assist;
– should realize that urgent assistance is important;
– should avoid blaming/teasing;
– should be familiar with local instructions and guidelines for “psychological first aid”.

17 Outsourcing

Given the increasingly complicated technical equipment required for ensuring optimal safety of cash transports, and with the number and violence of crimes against such transports on the rise, it has become widespread practice to outsource the task of transporting cash to private companies.

The decision to outsource the task is normally motivated by:

– savings on the investment side;
– insufficient in-house knowledge and capacity;
– a desire to minimize the risk of crimes against own staff; and
– changed transport flows.

In order to provide a fair basis for the evaluation of potential tenders, a detailed invitation to tender dossier should be prepared.