7.3 Cash security

Although the widespread adoption of digital money has generally reduced the amount of cash that organisations need to hold and handle, in many contexts and circumstances it is still necessary to hold, move and make transactions in cash. This chapter concerns multiple aspects of cash security, from theft and robbery to risks associated with cash programming.

7.3.1 Risks

While cash-related risks and their management are often the responsibility of finance and managerial staff, cash-related activities carry with them significant security risks. Withdrawing or transporting large amounts of cash makes aid workers vulnerable to robbery and theft. Travelling with cash, especially in remote or conflict-affected areas, increases the risk of being targeted by criminal elements or armed groups. The security risks of cash programming also need to be considered and addressed, including risks around transferring funds to aid recipients, fraud and reputational damage.

7.3.2 Risk mitigation measures

An essential first step is to carry out a risk assessment on the flow of cash around the organisation, followed by the design and implementation of mitigation measures at points of high risk.

The following section highlights measures to address risks associated with cash-related activities. These should ideally be decided and implemented collaboratively by security and finance staff.

Reducing the use of cash

Organisations can reduce their use of cash by making payments by cheque, bank transfer, pre-paid cards, credit cards or other electronic payments. No method of payment is risk-free, and it is important to establish guidelines on using credit cards and monitoring these regularly. Organisations dealing with sizeable transactions should consider taking out insurance specifically against loss or theft.

Risks of electronic transactions

There are several ways to transfer money without the use of cash. The risks associated with these mechanisms relate more to financial, operational or digital security, though there can be knock-on effects on staff security, for instance if a delayed transfer causes friction with parties expecting payment. Digital money transfer services and mobile apps can be vulnerable to hacking, phishing attacks and other forms of fraud and cybercrime. Informal systems known as hawala came under pressure post-9/11 over concerns that some transactions assist in the illegal transfer of funds to proscribed groups. Counter-terrorism legislation and bank de-risking practices have placed additional burdens on organisations trying to move large sums of money, in some cases forcing organisations to revert to using cash.

One specific risk around electronic financial payments is the targeting of transfers from donors to organisations or payments within organisations. Criminals are aware that very large sums of money are sent from donors to operational organisations, and also between head office and programme offices. Criminals could intercept email exchanges, clone staff accounts and issue false instructions to divert payments to external bank accounts. Last-minute changes or instructions in relation to significant bank transfers can also indicate fraudulent activity.

▶ *See Chapter 6.2 for more mitigation measures around digital security risks.*

Exercising discretion

When dealing with cash, discretion is important. The fewer people who know, the lower the risk. Communications that can be intercepted can be changed into some form of code. If withdrawing money from a bank, the transaction should be arranged discreetly in advance; avoiding making withdrawals at regular times or on regular days (e.g. in advance of monthly salary payments) can reduce risk. Paying suppliers is best done using one of the non-cash methods mentioned above, particularly for large sums. If staff regularly use the same hotel or supplier, organisations can consider setting up an account.

In some economies, and in cases of hyperinflation, the sheer bulk and volume of cash can present a problem. Even relatively modest amounts of international currency can translate into substantial bundles of local notes. When withdrawing cash from a bank, staff can try to have money paid out in higher denomination notes, and should consider the practicalities of transportation and storage.

Guidance for staff on good practice in cash security

- Do everything possible to limit the use of cash.
- Ensure reasonable credit limits and cash withdrawal limits.
- Check bank statements and investigate any unrecognised payments.
- Keep lists of phone numbers to call in case of loss or theft of credit cards.
- Block or cancel a credit card as soon as it is lost.
- Keep PINs safe.
- Keep credit cards in sight when handing over to pay for a purchase.
- Do not resist when confronted by a robber.

Limiting exposure

There are several ways to reduce exposure to loss or theft. Just-in-time payments to suppliers reduce the amount of time cash is held in the office. Another common practice is to set a ceiling on the amount of cash that can be withdrawn, transferred or kept in the organisation's safe. However, reducing the size of individual transactions will probably increase the number of transactions that need to be made, increasing costs. If cash is at most risk when it is being physically moved, organisations should consider moving larger amounts less frequently, particularly if more secure ways of transporting it are periodically available, such as helicopter flights or large convoys. Organisations can also consider the risks at different points in the transfer chain, from the bank to the organisation's safe to the eventual recipient, and represent this chain in a flowchart. It may be possible to reduce the number of links in the chain, for instance by asking suppliers to come to the office to receive payment rather than taking cash to them.

If burglary and robbery are risks, it is advisable not to keep all the money in one place, and have a certain amount to hand in an obvious place to satisfy and distract robbers. Some money should be easily accessible; the rest is better hidden. When travelling, staff should be encouraged to carry cash in different places and among different staff members travelling. In periods of high tension, when withdrawal, relocation or evacuation might be necessary, cash can be distributed among departing staff, partly to spread the risk and partly to ensure that staff have some cash to hand in case they become separated. Organisations should check that staff are comfortable with carrying large amounts of cash on them in situations of high tension or while travelling.

In countries where relocation or evacuation is a strong possibility, movements of cash should be prearranged and planned. The cash requirements of staff who may need to remain in place should be considered and addressed.

Case example: Sudan

In Sudan, one organisation needed to issue cash regularly as ‘emergency’ money for travel to local offices. To reduce the visibility and vulnerability of the cash, an amount of paper cash was placed between two sheets of paper (or a folded single sheet), and this was placed inside a special plastic pouch and laminated. Written instructions and a dotted line were printed on the paper in advance. This made a neat and protected package of pre-counted money. It also made accounting easier as there was no need to count the cash when it was issued and returned as long as the pouch was intact.

Reducing predictability

Routine increases risk, so organisations should try to avoid predictability in cash-related activities. Some common predictable risk points include:

- The monthly payroll.
- Special payments to staff prior to relocation or evacuation.
- Staff arrivals at airports and hotel/office transfers (thieves may monitor the arrival times of certain flights and may target vehicles on the main route into town).

- Trips by staff from the office to the bank and back, especially if they use the same route and travel at roughly the same time of day.
- Trips to the bank that involve more than one staff member may indicate that a larger than normal sum of money may be about to be deposited or withdrawn.

Extra security precautions can reduce predictability. For instance:

- Using an unmarked rented or local vehicle or a less obvious route to bring staff from the airport to the office or hotel.
- Changing salary periods and payment times, although this is unlikely to be popular with staff.
- Authorising a variety of staff members to go to the bank, changing routes and travel times.

Reducing vulnerability

Organisations can put in place measures to reduce vulnerability around cash, including guidelines around travelling with cash and site security measures.

To reduce vulnerability when transporting cash by road, at least two people, and preferably more than one car, can be involved. It is best to avoid predictability, and this may involve varying the number of passengers and cars used. In extreme cases, an armed escort or an armoured vehicle might be used, though this is likely to attract unwanted attention. When withdrawing cash from an ATM, a machine in a busy street with a queue of others waiting to do the same may be the most secure option. Staff should ideally withdraw money during the day and in company with a colleague to keep an eye on the surroundings. Staff may be observed taking out cash and might be followed, and so should avoid quiet streets or more dubious areas after visiting an ATM.

At the office, organisations can consider installing safes and having robust site security measures in place. Some considerations for safe security include:

- Anchoring the safe to the floor, and placing it in a back office or behind a desk so that it is hidden from visitors.
- Fitting a lock that requires two keys to open and giving the keys to two separate people, or using a key and combination lock.
- Being prepared in the event that robbers threaten violence against staff if the safe is not opened on demand (such as advising staff to hand over the keys or the combination if they are threatened).

- If a key holder is about to go away or on leave, ensure that a proper cash count is done with a new key holder, signed off by both parties.

▶ *For more information on site security, see Chapter 7.2.*

A note on identity theft

Identity theft and financial fraud, including credit card fraud, are large and growing problems. Some of the most common forms involve:

- Physical theft of cards and cheque fraud (printing fake cheques or stealing cheques).
- ‘Dumpster diving’ (stealing financial documents from the trash).
- Account redirection (fraudulently filling out a change-of-address form).
- Snatching a wallet or purse.
- Detaining individuals, including in their homes, while accomplices take their credit cards and PINs to a nearby ATM.

7.3.3 Cash programming

Many aid organisations have adopted cash programming as one of their main modalities for assisting people in crisis. The transfer mechanism can take various forms, such as digital transfers or vouchers, but can also involve the distribution of physical cash. The distribution mechanism should be appropriate to the context and consider practical constraints and security risks. Using banks and other financial institutions potentially reduces the security risks associated with cash transfers.

In general, when moving and storing cash for cash programming activities, many of the mitigation measures previously listed apply. Proper risk analysis, mitigation measures and monitoring are crucial. It is advisable for staff to carry out a programmatic risk assessment considering all the security risks to organisations, staff and aid recipients before and during the cash programme. Staff are not the only ones at risk when handling the cash: it is not uncommon for criminal groups to target and rob recipients of cash programmes. Cash distribution sites are also locations of high risk and will likely require appropriate site security measures.

There are also risks associated with the storage of beneficiary and financial data. Some organisations employ third-party data management tools to store and manage data. The potential data security and reputational risks associated with using such tools will need to be assessed prior to adoption.

Examples of risk mitigation in cash programming

In Afghanistan and Somalia, organisations have successfully used local remittance companies to deliver money to people in remote and insecure areas.

In Ethiopia, one international organisation took out insurance coverage against the risk of loss in transporting cash to projects in areas where there were no banks.

In Zambia, an international organisation sub-contracted delivery in remote rural areas to a bank and financial services group, which used security company vehicles to deliver the cash, accompanied by local police.

The transfer of cash on a wide scale creates institutional risks related to fraud, diversion and misappropriation. There are also compliance risks in relation to counter-terrorism legislation and donor sanctions in high-risk environments. These risks are often seen as more serious than if they were to happen with in-kind aid, and should be carefully considered, prepared for, mitigated and responded to. The reputational damage of any fraudulent activity relating to a humanitarian organisation's operations can have serious consequences (see case example below).

Case example: Turkey

In 2015, an investigation by USAID uncovered fraud involving several individuals, some working for NGOs, in cross-border humanitarian aid from Turkey to Syria. The investigation found major corruption in the procurement process, including bribery, bid rigging, kickbacks and collusion between NGO logistics staff and corrupt commercial vendors. At least one international NGO staffer faced criminal charges and extradition, and the NGOs involved suffered severe reputational damage among their donors and the broader public. The massive volume and rapidity of funding flowing to international NGOs in Turkey, which were under pressure to ramp up operations quickly, was a factor in inadequate financial controls, procurement procedures and vetting requirements.

Source: Parker, B. (2018) 'US bans aid workers in Turkey-Syria scam' The New Humanitarian, 11 September (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

Further information

Guidance, tools and discussion

Cornish, L. (2017) 'New security concerns raised for RedRose digital payment systems' Devex, 28 November (www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619).

ICRC (2021) *SAFE: Security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

International Red Cross and Red Crescent Movement (n.d.) 'CTP risk matrix template'. Module 3, Step 1, Sub-step 4, Cash in emergencies toolkit (https://cash-hub.org/guidance-and-tools/cash-in-emergencies-toolkit/all-toolkits/).

Parker, B. (2018) 'US bans aid workers in Turkey-Syria scam' The New Humanitarian, 11 September (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

The CALP Network (n.d.) Key resources (www.calpnetwork.org/key-resources/).