

17th European Report on Bank Robberies

Executive summary

1. Foreword

The problem of robberies is constant and will remain as long as money exists. This is frequently accompanied by a change in the *modus operandi*.

The criminal threat also seems to be influenced by the economic situation in the country concerned or in neighbouring countries. During the 21st annual meeting of the Physical Security Working Group held in Tallinn on 9 June 2009, attention was again focused on Bank raids. An analysis, based on a statistical and practical exchange of information, was made of the financial institutions' exposure to criminal actions. Topics discussed in depth included violent attacks, such as raids on bank branches, ATMs and cash in transit.

Within the framework of these discussions, the Working Group tried to detect the general tendencies in the field of bank security, as well as the new developments and the countermeasures. This exchange of information aims to achieve a better understanding of new risks and to elaborate more appropriate countermeasures.

The detailed analysis of the 2008 statistics on bank robberies has brought to light some general tendencies. First, the drop in the number of robberies seen in 2005, continued significantly in 2008. Nonetheless, even though total losses were significantly lower, the average amount stolen has barely changed and is still considerable.

Second, the risks are evolving. The increase in the range of risks, identified a few years ago, to which branches are vulnerable to attack is becoming more and more widespread. Traditional ways of operating are still used but new ones are developing. The focus of criminal activities remains centred on ATM raids and the increase in violent ways of operating continued throughout 2008 ('tiger kidnapping', gas attacks on ATMs, etc.). The use of violence is reported in nearly every country, in raids committed by both amateurs and by professionals.

a.i.s.b.l. The amateur robberies were most frequent in 2008, and were frequently

accompanied by violence, especially firearm endangerment. In professional robberies, the personnel are generally kept under threat for longer periods, with a greater physical and psychological impact. As a result, victim support is provided for both staff and customers in almost every country.

Moreover, the desire to relieve banking personnel of tasks linked to the treatment of cash, has led to a gradual modification of the *modus operandi*. The number of ATMs' robberies and subsequent damage caused, significantly rose in 2006, and remained high in 2008. The 2007 trend in ATMs' attacks using fraudulent means of extracting cash reveals an increasing number of successful attempts in 2008. Nonetheless, ram raids and explosions on ATMs, less numerous than fraudulent extractions, cause more significant losses.

Another trend is the worrying development of e-crimes. 2006 is considered as the worst year so far, though in 2008 the level of e-crimes remained high, and new methods appear.

2. Trends

The robbery situation varies greatly from one country to another. Nevertheless, broadly speaking, some trends can be observed.

2.1 Number of Robberies

In 2008, 4726 bank robberies were committed, 15% fewer than in 2007. The number of robberies committed differs from one country to another.

The risk rate which provides an objective standard also varies considerably between the countries. The highest rate was 1/13 followed by 1/16. The lowest risk rates were in 1/418 and 1/411. In 2008, risk rate amongst the EBF member countries amounted to 1 to 54 (as compared to 1 to 37 in 2007).

2.2 Target – The rapidly evolving branches

In most countries the number of branches continues to fall, owing to the policy of enhancing the efficiency of services provided, by promoting the use of electronic banking.

Owing to security reasons, cost efficiency and the wishes of customers to have round-the-clock banking services and a 24-hour economy, cash is increasingly dispensed through ATMs. More and more ATMs are installed off-premises.

The trend of installing money boxes in shops or public areas is continuing. In some countries, over half of the ATMs are located in supermarkets. These ATMs are operated in a variety of ways: either the bank is the owner and rents space, or the ATM is operated by the bank and the retailer together for their joint account. There are also joint ventures between retailers and, for instance, cash-in-transit operators.

Cash handling is increasingly being outsourced to specialised companies. This is done not only for efficiency or cost reasons but also in view of the security risks.

Nonetheless, the bank branch currently still remains one of the biggest distribution channels, but is also evolving in terms of concept.

Furthermore, in some countries, the desire to limit operations with little added value has led to a progressive transformation of certain bank branches. This trend has made banks turn towards branches that are more specialised in giving advice and are sometimes even cashless. Consequently, the number and use of ATMs keeps rising. Other types of machines are also appearing: cash recycling machines, machines for cash depositing or dispensing, cheque processing, etc. In such branches, more than before, funds intended for, or originating from clients, are concentrated in the special areas where the different machines are located.

As a result, it is logical that the number of direct attacks (by means of fraudulent extraction, explosives, gas, etc.) but also indirect (threatening of employees to make them open up the ATM safes, attacks when the ATM is being supplied with funds, etc) will continue to increase in the future. ATMs are a popular target for professionals because of the large amount of money to be found. Similarly, ATM frauds, such as skimming, were as numerous in 2008 as in 2007. As for the attacks (with no physical aggression) against the ATM Network (skimming or card trapping), the number is slightly decreasing.

The other significant trend identified a few years ago, is to take on softer targets such as bank employees in order to get around the security devices, usually highly sophisticated in banks. The criminals directly attack bank employees or members of their family and force them to deactivate the existing security devices in order to get at the cash. 'Tiger kidnappings', kidnappings and home

invasions occurred in 2008 in several countries though their number is not significant.

As for the targets, it has also been pointed out that bands of criminals often attack the same bank systematically using often the same technique.

2.3 Perpetrators

It is difficult to gather precise information about the people committing robberies and other aggressions towards banks. However, some trends can be observed.

Although tendencies may vary from one country to another, raiders generally can be divided into two major groups. On the one hand, the **professional-type raider**, well prepared, often using extreme violence and tailor-made means, targets large amount of money. On the other hand, there is a growing group of **amateurs** (69% of robbers in 2008). They tend to be satisfied with smaller booty, than professionals, but nonetheless remain dangerous as they also use weapons.

The percentage of amateurs and professionals varies from country to country. The general tendency of a higher number of amateurs has remained so for years.

This is reflected in the number of perpetrators *per* raid. On average, **54%** of the robberies were committed by one perpetrator, **27%** by two, and **10%** by more than two perpetrators.

In some countries the robbery population consists of a disproportionate number of foreigners. This complicates the investigation as the raiders are not known in the country of crime, and after striking usually quickly depart elsewhere. With this in mind, a coordinated cross-border approach by the European police authorities should be given due attention.

The number of raids increases significantly following the success of given groups of raiders committing series of crimes. Success often attracts other potential criminals and the experience gained during earlier raids is passed on within the groups, resulting in imitations of successful raids. Thus, the security measures implemented by banks as well as police action and vigilance are crucial in discouraging potential raiders. Indeed, the number of arrests influences the amount of attempted attacks.

An alarming trend is the continuing increase in the use of violence during raids. Some perpetrators do not hesitate to take more risks with regard to the means employed, e.g. explosives, which are difficult to handle. Serious and prolonged threats evidently carry considerable risks to the physical integrity of the employees and clients aside the significant psychological impact. This type of aggression is more common with organised gangs that prepare their raids in order to obtain larger amounts. Nonetheless, these groups are still slight compared to the number of amateurs.

2.4 Protective countermeasures

Protective countermeasures are aimed at anticipating and limiting risks as much as possible, especially for the bank employees and clients. The most effective measure to fight bank robberies is police intervention. In countries where the police actively concentrate on groups of raiders, the robbery statistics are falling. Penalising those committing series of robberies, seems to be the best prevention.

In many countries, depending on the risk situation, use is made of **camera surveillance**, sometimes visible, sometimes a combination of visible and non visible, sometimes aimed at, or placed near the ATM, often covering the entrance. Another effective tool is a delaying system in combination with **alarm systems**. This increases the chances of the police arresting the raider. However, the alarm is not set off until after the incident. Raiders can be tracked down through a transmitting device hidden amidst the banknotes stolen.

An overall review of protective measures has shown that **metal detectors** are used to a limited extent and in only few countries. Surveillance cameras are used in many countries to a greater or lesser extent, in all lines of business. **Attack alarms** are used in every country. This also applies to **burglar alarms**.

In order to help police investigation, it is also useful to provide the personnel with post-incident instructions e.g. not to clean up so as to leave any traces such as DNA; give a good description of the perpetrators etc.,). Procedures for this may be determined in advance in collaboration with the police.

In addition to investigative tools, it is important that, for each individual bank office, a proper alarm, communication, and attack plan is prepared in collaboration with the police. While reducing the chances of an escalation of attacks, it increases the chances of arresting the perpetrators. An effective attack

plan is based on a policy of prompt alarm, contact with the object for verification, encirclement of the premises, and entry of the premises forbidden until there is certainty that the raiders have left.

In some countries the protection of the cashier area by means of bullet-proof (and burglar-proof) glazing remains customary, in spite of a developing trend towards more open offices. In the latter cases, banks try to limit employees' access to cash as much as possible. In several countries **cash dispensers** are therefore used. The principle is based on 'cash dispensation independent of staff' subject to certain limitations. The 'teller' machines are only allowed to issue limited amounts *per* time unit. So the 'tellers' are no longer the key to the money. Access to vaults or ATM safes may also be limited (time delay, distance opening).

Limiting access to cash is also a countermeasure for early morning hold-ups or hold-ups by kidnapping. To limit these risks, procedures for opening safe-deposit boxes in vaults, etc. could be implemented, featuring dual control, separation of consignments, delaying systems, distance opening. The aim is to prevent one single person from having access to large funds. In the fight against hold-ups, some banks have also installed one-person locks (e.g. only one person at a time can enter the protected area, thus disabling hostage taking). With this in mind, subcontracting may also offer solutions, e.g. because the personnel no longer has access to the ATMs, and the maintenance of those ATMs is sometimes given to cash in transit firms. Be that as it may, in such cases, it is imperative that banks define preventive security measures with their subcontractors. Otherwise, attacks on the subcontractor will inevitably have direct (cash distribution) or indirect (legal intervention) repercussions for the bank.

In order to prevent ATM raids, the technical areas must be protected against forceful entries. This protection should be able to hold, for at least as long as it takes to detect the entry, and to react to the crime (by sending of a guard notifying the police). The above protection should be complementary to the protection of the ATM safes, which have to be securely anchored into the ground. Attacks on the ATM safes, by means of extraction (e.g. the ATM hauled out by a fork-lift truck or by use of a lorry and a steel cable around the ATM) and use of explosives (or gas), are sometimes very spectacular and can cause serious damage to the surroundings. For this reason, in some countries, taking into account the limitations of physical security, ATMs are equipped with a

staining system for the bank notes (in the safe or the cassettes) in order to render the haul useless in case of a raid (the same systems are used for cash in transit).

Generally no use is made of **armed guards** at branches. Presence of arms can result in an escalation of violence. Guards can however play a role in access control, for instance in combination with revolving doors fitted with metal detectors. They also can play a role in creating an added sense of security among the staff after a raid, for instance at opening and closing hours.

Victim support is consistently in place in all countries (for staff and sometimes – on a limited scale – for customers).

2.5 Security transport

In 2008, there were **358** attacks reported against cash in transit (CIT) as opposed to 499 reported cases in 2007. Countries such as Germany, UK, and France are particularly exposed. The situation remains stable, but certain difficulties in gathering statistics on this type of raid occurred.

Against these often very violent attacks, (weapons of war, explosives, truck, etc), some countries have reinforced the security requirements for CIT. Among the tendencies observed, there is, in particular, a greater use of smart boxes that ‘neutralise’ the values in the event of attack), and aim to make unusable any hauls.

As a result, the additional security requirements applied to CIT could cause a shift of raids towards the bank branches, and other points of cash concentration. In certain countries, an increase can already be observed, for example, in the number of attacks on branches during, or right after the delivery of the funds by the CIT (the United Kingdom).

3. The future

Robbery analysis indicates that protection against robbery and burglary will require constant attention in the future. Criminals will always try to find means to circumvent the security measures taken by banks.

Furthermore, the upgrade of Public-Private partnership, i.e. between banks and the police as well as the judiciary, is an effective measure to cope with bank

crime. For this reason, security committees, banks, and the police actively have to develop their combined efforts in the investigation field, e.g.: immediate information sharing, coordination of security measures, etc.

The increase of **e-crimes** is another trend to be discussed in the future as well as the need for more efficient computer security systems. Indeed, there are more and more effective means to perpetrate “**e-bank raids**”, especially through criminal software available on the Internet. This issue requires an urgent attention from the bank and official security.

In conclusion, even if other channels of distribution have been developed over recent years, the **bank branch** remains the chief source of cash distribution (or cash distribution remains the main banking activity for bank branches). The branch concept will undoubtedly continue to evolve towards greater automation with regard to the deposit and withdrawal of cash with the number of **ATMs** continuing to increase. Banks are also expected to outsource their cash-handling.

All these changes contribute to the development of the branch concept, and constitute important new challenges for the banks’ security officers, not least as more and more monies are concentrated in cash tellers.