SECURITY

The concepts of banking and security are inseparable: first, since the handling of money directly exposes bank employees, customers and suppliers to risks, namely of assault and theft, second, because it was the need for security (as regards the deposit and circulation of money) that led to the emergence of banks, and lastly because it is the basis of banks' purpose and reputation. Security issues come in different forms, which can be grouped into three categories: physical security, notably regarding the transport of funds and security systems of bank branches; financial security, which concerns the fight against money laundering and the financing of criminal activities; and lastly technological security, linked to the development of dematerialised means of payment and the Internet.

PHYSICAL SECURITY: A PRIORITY FOR BANKS

Banking institutions spend large sums on security training and installations, which represent one-third of the cost of a new branch, while the total cost to the industry amounts to some EUR 230 million per year, excluding non-recurring investments linked to the French law of July 10th 2000. However, the application of this law and the French decree of December 18th 2000, which govern the refurbishment of branches and cash-in-transit systems, poses major problems.

Review the provisions of the French law of July 10th 2000

In response to the urgent situation created by difficulties in applying the French law of July 10th 2000, the French law on internal security of July 13th 2002, tacks on an additional year to the original timetable for refurbishing bank branches, where banks have submitted an application to the administrative authorities.
That said, the French law of July 10th 2000 and its related decree of December 18th still contain serious flaws:

- they only concern a limited segment of the cash-in-transit chain, i.e. the distance covered on foot between the armoured car and the bank branch, thus transferring the risk of assault up or down the chain;
- in principle, they encourage "Maginot line" techniques: reinforcing the heavy shielding and security fittings on bank branch façades, while some of the more modern and more dissuasive alternative security techniques (see inset) are only used on an exceptional basis;
- they treat all branches indifferently, regardless of their location (city centres or less densely populated areas), degree of protection or exposure to risks;
- they require heavy and complex administrative procedures, which are often unclear, in order to obtain the necessary prior authorisation to refurbish branches but fail to coordinate the works of the different parties involved (local security authorities, town councils, local building authorities, co-ownerships, etc.);
- lastly, ambiguity in the legislation leaves loopholes to avoid criminal prosecution.

The banking profession's proposals to improve security

An interdepartmental team, set up in the second half of 2002, is scheduled to produce a report assessing the entire cash-in-transit chain in the spring of 2003. The FBF would like these findings to contribute to progress in this area and to be used in developing the most appropriate solutions for the security of all those concerned. The Federation put forward its proposals at two separate hearings:

1) limit the number of deliveries by "recycling" cash in bank branches;
2) loosen the restrictions on the use of "alternative security systems", by eliminating the legislative provisions which confer them with an exceptional status;
3) in collaboration with the public authorities, implement a permanent, all-encompassing security plan for the entire cash-in-transit chain, along the lines of the security measures adopted during the changeover to the euro.

The number of hold-ups in bank branches fell from 937 in 2001 to 759 in 2002.

BANKING NETWORKS AND "ALTERNATIVE" CASH-IN-TRANSIT SYSTEMS

An increasingly common mode of transport

Alternative cash-in-transit systems have undergone constant development since their beginnings in 1990. Today, their prospects look promising with new possibilities for implementing these solutions. The banking sector would like to maintain a gradual development in order to allow the end-users and cash transporters to adapt to the system under optimal conditions. Banking networks use both modes of transport that exist today, armoured cars with armed men or unmarked vehicles equipped with systems that automatically destroy the notes. Today, approximately 60% of the banking network sites receive funds via alternative cash-in-transit systems. They ensure security in a variety of situations, particularly at a geographical level and offer the advantage of flexibility in terms of logistics, as they can be adapted to the volume transported, the type of journey and the branch location. They have also proven their effectiveness in terms of security. Specialists believe that they reduce the risk of violence linked to an escalation in armed measures. These systems are considered less stressful for both the branch staff receiving the funds and customers who feel ill-at-ease during deliveries by armed men.

Ill-adapted regulation

By referring to the use of unmarked vehicles equipped with a system for rendering the notes worthless (cash-staining solution currently used) driven by an unarmed man as "exceptional", the decree of November 20th 2002 does not ensure equal treatment of the different modes of transport and consequently does not guarantee the end-users the freedom of choice. Banks would like to be able to choose the mode of transport that is best suited to their needs with comparable levels of security and lament that this new regulation was passed before the interdepartmental team on cash-in-transit could present its findings.

Limiting the risks: recycling cash in ATMs

The entire banking profession is in favour of recycling cash, i.e. filling Automatic Teller Machines (ATMs) with cash deposited by customers following an authenticity check. This option would reduce the volume of cash in transit, and therefore limit the risk of assault. The European Central Bank has come out in favour of the recycling of notes in machines.

THE FIGHT AGAINST MONEY LAUNDERING, ORGANISED CRIME AND TERRORISM

* The number of declarations sent to Tracfin has risen from 179 in 1991 to 1,655 in 1999, 3,598 in 2001 and 6,896 in 2002.

Over the past ten years, anti-money laundering and anti-terrorist financing measures have become a major priority for banking institutions. In 2002, clarifications on cheque authenticity have completed the general rules stipulated by the anti-money laundering legislation, which is based on the fundamental principle of "Know Your Customer" (NRE law of 2001).

2002: new regulations on cheques

Ambiguity in the legislation with regard to banking practices prompted the Comité de la Réglementation Bancaire et Financière (CRBF – French Banking and Finance Regulation Committee) to clearly set out the banks' obligations with regard to cheques as part of the fight against money laundering and terrorism in Regulation No. 2002-01. This legislation transposes into regulations the findings of an interdepartmental working group set up in collaboration with sector professionals. It meets the need for greater efficiency in detecting illegal financing via cheques in an environment marked by the internalisation of financial flows and the use of new technologies. In particular, banks must implement an annual cheque control system, which notably takes into account the types of money laundering and the information released by the FATF (Financial Action Task Force). The legislation reinforces and clarifies the obligations to control cheques from abroad. Cheques requiring multiple endorsement from countries on the FATF's black list should be controlled systematically.

As an initial step in the anti-money laundering measures, 25% of cheques from countries which are not members of the FATF but do not figure on the black list will be subject to verification. The new regulation prohibits French banks from accepting cheques cashed abroad, which are sent to them by banks to which they are not bound by an agreement. Furthermore, French banks will have to impose strict contractual obligations on their partners and check that these obligations are met. Compliance with these provisions will be verified by the Banking Commission which has the authority to punish any non-compliance based on its general disciplinary authority.

THE OBLIGATIONS OF BANKS

Reporting rules

Under the French laws of 1990 and 1993, banks must report any suspicious transactions to Tracfin. Reports of suspicious acts must relate solely to money laundering from drug trafficking or organised crime.
In 2002, banks made 6,896 declarations to Tracfin, nearly twice the number made in 2001.
In 2001, the French law on new economic regulations ("NRE law") set out new requirements to systematically report both transactions where there is still doubt as to the customers' identity (principal or beneficiary) after verification and transactions carried out with trust funds.

Customer identification rules

- The identity of any customer who asks to open an account must be checked and the related records kept for 5 years;
- The identity of any occasional customer who requests a safety deposit box or carries out a transaction involving more than EUR 8,000 (FRF 50,000) must be checked and the related records kept for 5 years;
- If it appears a person may not be acting on his/her own behalf, the true identity of the person on whose behalf he/she is acting must be checked;
- A special register must be kept listing the identity of persons who carry out transactions involving anonymous bonds and securities and gold transactions.

Rules on large, unusual transactions

- Any large transaction carried out under unusually complex terms and without any apparent economic justification or legal purpose should be subject to special examination. The banking institution is required to investigate the origin and destination of these sums, the purpose of the transaction and the identity of the beneficiary.

Other obligations

Banks must implement internal written procedures to be followed in order to comply with their obligations. They should train and inform their staff. Lastly, they should ensure that their subsidiaries and branches abroad comply with these rules unless the local legislation prevents them from doing so, in which case they must inform Tracfin.

TECHNOLOGICAL SECURITY

With the development of technologies (means of payment, online banking) the security of transactions is a permanent concern for banks.

In 2002, the record level of bank card transactions marked the end of the predominance of cheques as a means of payment. For example, with over 4.8 billion transactions, the "CB" system has become the leading dematerialised payment instrument in France.

French banking institutions spend an average of over EUR 150 million every year on maintaining and improving the security of bank cards.

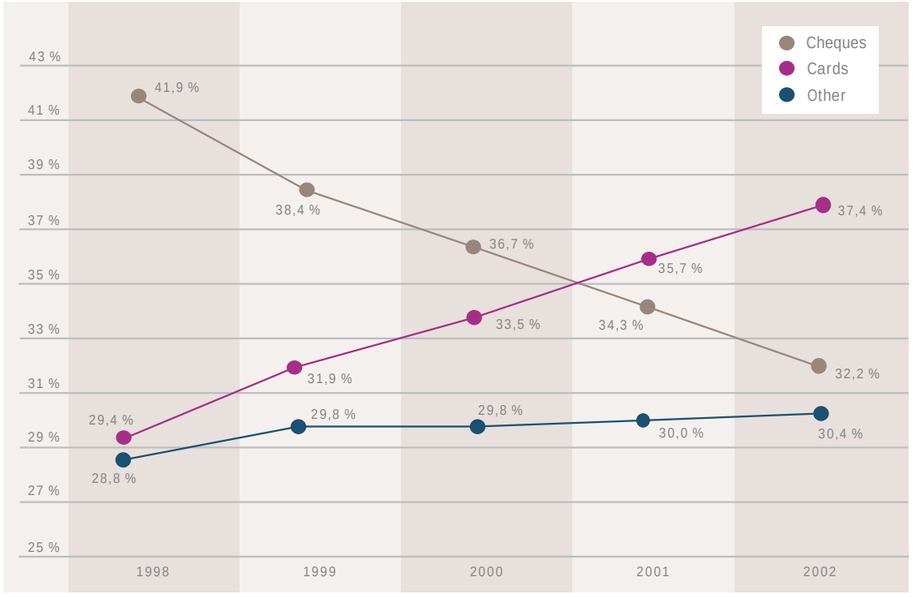
Over the past few years, they have developed a vast programme to modernise the entire electronic payment system, with a dual objective:

- implement a more flexible authorisation network that offers higher levels of security for bank card transactions;
- adapt cards, payment terminals and ATMs to the new generation of smart cards, thus reinforcing the security system.

Moreover, the law on everyday security gave rise to committee responsible for supervising the security of all payment cards in use in France. Committee members and their scope of competence were set out in a decree at the end of 2002. A representative from the FBF participates in the work carried out by this Committee, whose mission is to propose means to combat technology-based attacks on the security of card payments".

USE OF MEANS OF PAYMENT

Number of transactions carried out by cheque, bank card or other means (direct debit, electronic bill of exchange)



Card and cheque transactions include payments and withdrawals.

INTERNET SECURITY

The findings of a working group which brought bankers and security specialists together within the FBF were compiled in the Banking Information Centre's Mini Guide No. 4 on best practices in terms of security for Internet transactions, at the level of both banks and customers.

Best practices for THE BANK

- **Facilitate access and transactions:** offer 24/7 access where possible; provide details of all transactions online; offer an acknowledgement of receipt for all Internet transactions; request confirmation before registering orders.
- **Ensure a high level of security:** make access secure, at least with a user name and password; allow customers to change their password at any time; allow customers to block their access to the service; offer a secure transmission system; display the date and time of the last connection; advise or even require the use of a browser with an adequate level of security; display a button to exit the online banking service on all pages; automatically disconnect if no transaction has taken place.
- **Describe the functions and uses:** offer an online presentation of e-banking services; indicate the means and terms of access to online banking helpdesk; present the site's security policy.
- **Present the possible courses of action in case of dispute:** explain procedures; undertake to refund any transaction wrongly debited to the customer's account, following investigation.

Best practices for THE CUSTOMER

- **Safeguard PIN code:** keep PIN in a safe place; do not save it automatically on the computer; do not record it where it is easily visible; do not give it to anyone; change it immediately upon registration with the service, then change it regularly; do not use an easily identifiable PIN.
- **Take necessary precautions:** use the manual disconnect buttons immediately following consultation rather than wait for automatic disconnection; be particularly careful when using any self-service PCs (see the special recommendation below); use a regularly-updated anti-virus tool; take appropriate measures for computers with permanent internet connection.
- **Inform the bank of any irregularities:** immediately inform the bank of the loss or theft of information enabling access to the online banking service; regularly check your accounts; immediately inform the bank of any irregularities.
- **Stronger precautions for users of self-service PCs,** which may store information even after you have logged out.