LA SÉCURITÉ

Les notions de banque et de sécurité sont indissociables : d'abord parce que le maniement de l'argent expose directement les collaborateurs, les clients et les fournisseurs des banques à des risques, notamment d'agression et de vol ; ensuite parce que c'est la recherche de sécurité (du dépôt et de la circulation de l'argent) qui a "fondé" les banques ; enfin parce qu'il y va de l'utilité et de la réputation des entreprises bancaires.

Les questions de sécurité prennent des formes différentes, qu'on peut regrouper en trois catégories : la sécurité physique, notamment pour le transport de fonds et l'aménagement des agences bancaires ; la sécurité financière, qui porte sur la lutte contre les circuits de blanchiment et les modes de financement des activités criminelles ; la sécurité technologique enfin, liée au développement des moyens de paiement dématérialisés et de l'Internet.

LA SÉCURITÉ PHYSIQUE : UNE PRIORITÉ DES BANQUES

Les entreprises bancaires consacrent des sommes importantes à la formation et aux aménagements de sécurité : 1/3 du coût d'une nouvelle agence, et globalement pour la profession, de l'ordre de 230 millions d'euros par an, hors les investissements exceptionnels consécutifs à la loi du 10 juillet 2000. Toutefois, l'application de cette loi et du décret du 18 décembre 2000 qui régissent l'aménagement des agences et le transport pose des problèmes majeurs.

Revoir les dispositions de la loi du 10 juillet 2000

Devant l'urgence de la situation créée par les difficultés d'application de la loi du 10 juillet 2000, la loi sur la sécurité intérieure du 13 juillet 2002 reporte d'un an le délai prévu pour la réalisation des travaux d'aménagement des agences bancaires dès lors que les banques ont déposé un dossier auprès des autorités administratives.
La loi du 10 juillet 2000 et son décret d'application du 18 décembre demeurent en tout état de cause marqués de graves défauts de conception :

- ils ne concernent qu'un segment étroit de la chaîne de circulation de l'argent : celui du trajet piétonnier entre le véhicule de transport de fonds et l'agence bancaire, déportant de ce fait les risques d'agression en aval ou en amont ;
- ils privilégient par principe les techniques de "ligne Maginot" : renforcement des blindages et aménagements lourds en façade des agences bancaires alors que les techniques plus modernes et plus dissuasives des moyens alternatifs (cf encadré) n'y font l'objet que d'un traitement par exception ;
- ils traitent de manière indifférenciée toutes les agences, quels que soient leur localisation (centres-ville ou milieux diffus), leur degré de protection ou leur exposition aux risques ;
- ils instaurent, au demeurant de manière souvent imprécise, une procédure administrative lourde et complexe en préalable nécessaire aux réalisations de travaux et font intervenir de façon non coordonnée les différentes parties concernées (commissions départementales de sécurité, municipalités, D.D.E., copropriétés…) ;
- enfin, sur le plan juridique, ils laissent subsister des ambiguïtés incompatibles avec le dispositif de sanctions pénales.

Les propositions de la profession pour améliorer la sécurité

Une mission interministérielle, mise en place au second semestre 2002 pour dresser un diagnostic global sur l'ensemble de la filière fiduciaire, doit remettre un rapport au printemps 2003. La FBF souhaite que ses conclusions permettent de progresser et de trouver les solutions les plus appropriées pour la sécurité de tous. Auditionnée à deux reprises, elle a fait part de ses propositions :

1) limiter le nombre de transports de fonds par le développement du recyclage sur place des espèces dans les agences bancaires ;
2) assouplir les conditions d'utilisation des "moyens alternatifs" en supprimant certaines des contraintes fixées par les textes qui leur confèrent un statut d'exception ;
3) mettre en place, en concertation avec les pouvoirs publics, un plan permanent et global de sécurisation de la chaîne de circulation de l'argent, à l'instar de ce qui a été fait au moment du passage à l'euro.

Le nombre d'agressions dans les agences bancaires est passé de 937 en 2001 à 759 en 2002.

LES RÉSEAUX BANCAIRES ET LE TRANSPORT DE FONDS "ALTERNATIF"

Un mode de transport de plus en plus utilisé
Depuis leurs débuts en 1990, les systèmes alternatifs n'ont cessé de se développer. Ils offrent aujourd'hui des perspectives prometteuses avec de nouvelles possibilités d'application. La profession bancaire souhaite pour sa part que cette évolution se fasse de façon progressive pour permettre aux donneurs d'ordre et aux transporteurs de fonds de s'adapter dans les meilleures conditions possibles. Les réseaux bancaires utilisent concurremment les deux modes de transport de fonds qui existent aujourd'hui, les blindés avec hommes en armes, ou les véhicules banalisés équipés de systèmes de destruction automatique des billets.

Aujourd'hui, environ 60 % des sites des réseaux bancaires sont desservis par le transport de fonds alternatif. C'est une moyenne qui recouvre des situations assez différentes, notamment sur le plan géographique. Le transport alternatif a l'avantage de la souplesse en termes logistiques. Il peut s'adapter aux volumes transportés, aux types de trajet ou de localisation des agences. C'est aussi un mode de transport qui a fait ses preuves en matière de sécurité. Les spécialistes considèrent qu'il diminue les risques de violence liés à la surenchère de l'armement. Il est perçu comme moins stressant pour le personnel d'accueil, mais aussi pour les clients qui souvent s'inquiètent lors des dessertes par des hommes en armes.

Une réglementation inadaptée
En maintenant les termes "à titre exceptionnel" pour la solution en véhicule banalisé équipé d'un système de désinsertion des valeurs (actuellement maculage des billets) et conduit par un homme sans armes, le décret du 20 novembre 2002 n'assure pas un traitement égal entre les différents modes de transport et ne garantit donc pas la liberté de choix des donneurs d'ordre. Or les banques souhaitent pouvoir opter, à un niveau de sécurité comparable, pour le mode de transport le plus adapté à leurs besoins. Elles regrettent que cette nouvelle réglementation ait été décidée avant la conclusion des travaux de la mission interministérielle sur le transport de fonds.

Limiter les risques : le recyclage dans les DAB

L'ensemble de la profession bancaire est favorable au recyclage, c'est-à-dire au chargement des Distributeurs Automatiques de Billets (DAB) avec des billets remis par la clientèle et dont l'authenticité a été vérifiée. Cette possibilité permet de réduire les flux de circulation des espèces et donc les risques d'agressions. La Banque centrale européenne a pris elle-même position en faveur de l'usage de machines à recycler les billets.

LA LUTTE CONTRE LE BLANCHIMENT, LA CRIMINALITÉ ORGANISÉE ET LE TERRORISME

Au cours des dix dernières années, la lutte contre le blanchiment et le financement du terrorisme a donné lieu à une vraie prise de conscience et à des efforts importants de la part des entreprises bancaires. En 2002, des précisions sur la vérification des chèques viennent compléter les règles de vigilance générales prévues par la législation relative à la lutte contre le blanchiment, qui se fondent sur le principe fondamental de la connaissance du client (loi NRE 2001).

* nombre de déclarations adressées à Tracfin : de 179 en 1991, il passe à 1 655 en 1999, à 3 598 en 2001 et à 6 896 en 2002.

2002 : une nouvelle réglementation sur les chèques

Les ambiguïtés des textes, au regard des usages bancaires, ont conduit le Comité de la Réglementation Bancaire et Financière (CRBF) à préciser dans le règlement n°2002-01 les obligations de vigilance des banques au titre de la prévention du blanchiment et du financement du terrorisme en matière de chèques. Ce texte est la traduction réglementaire des conclusions d'un groupe de travail interministériel mis en place avec les professionnels. Il répond à la volonté d'améliorer l'efficacité de la détection des financements illicites par l'utilisation des chèques, dans un contexte caractérisé par l'internationalisation des flux financiers et l'usage des nouvelles technologies. Les banques doivent en particulier prévoir un programme annuel de contrôle des chèques tenant compte notamment des typologies du blanchiment et des informations publiées par le GAFI. Le texte renforce et précise les obligations de contrôle concernant les chèques provenant de l'étranger. Les chèques à endos multiples provenant des pays figurant sur la "liste noire" du GAFI devront faire l'objet de contrôles systématiques.

Ceux provenant des pays non-membres du GAFI mais qui ne figurent pas sur la liste noire feront l'objet de vérifications par des sondages ciblés dont le taux a été fixé dans une première étape à 25 %. Le nouveau règlement interdit aux banques françaises d'accepter les chèques encaissés à l'étranger qui leur sont transmis par des banques auxquelles elles ne sont pas liées par une convention. Les banques françaises devront en outre imposer à leurs partenaires des obligations contractuelles strictes et en vérifier la mise en œuvre. Le respect de ces dispositions sera vérifié par la Commission bancaire qui pourra sanctionner les éventuelles défaillances sur la base de son pouvoir disciplinaire général.

LES OBLIGATIONS DES BANQUES

Les obligations de déclaration

Aux termes des lois de 1990 et de 1993, les banques doivent déclarer à Tracfin toute opération qui leur paraît suspecte. Les déclarations de soupçon doivent porter uniquement sur le blanchiment d'argent provenant du trafic de stupéfiants ou d'activités criminelles organisées.
En 2002, les banques ont fait quelque 6 896 déclarations à Tracfin, soit près de deux fois plus qu'en 2001.
En 2001, la loi sur les nouvelles régulations économiques, dite loi NRE, impose de nouvelles obligations, cette fois sous forme systématique : elles concernent d'une part les opérations pour lesquelles l'identité du client (donneur d'ordre ou bénéficiaire) reste douteuse après vérification d'autre part, les opérations réalisées avec des fonds fiduciaires.

Les obligations de vigilance

quant à l'identité des clients

- vérifier l'identité de tout client qui demande l'ouverture d'un compte (et en garder la trace pendant 5 ans) ;
- vérifier l'identité de tout client occasionnel qui demande à louer un coffre ou à réaliser une opération supérieure à 8000 euros (50 000 francs) et en garder trace dans les mêmes conditions ;
- s'il apparaît que la personne pourrait ne pas agir pour son compte, se renseigner sur l'identité véritable de celui pour le compte duquel elle agit ;
- pour les bons et titres anonymes et les opérations sur l'or, création d'un registre spécial dans lequel est conservée l'identité des personnes qui effectuent ces opérations.

quant aux opérations importantes et inhabituelles

- procéder à un examen particulier de toute opération importante se présentant dans des conditions inhabituelles de complexité et ne paraissant pas avoir de justification économique ou d'objet licite. L'établissement de crédit a l'obligation de se renseigner sur l'origine et la destination de ces sommes ainsi que sur l'objet de la transaction et sur l'identité de la personne qui en bénéficie.

Les autres obligations

Les banques doivent mettre en place des procédures internes écrites à suivre pour se conformer à leurs obligations. Elles doivent former et informer les membres de leur personnel. Elles doivent s'assurer enfin que leurs filiales et succursales à l'étranger respectent ces règles, à moins que la législation locale n'y fasse obstacle, auquel cas elles doivent en informer Tracfin.

LA SÉCURITÉ TECHNOLOGIQUE

Le développement des technologies (moyens de paiement, banque en ligne) s'accompagne d'une réflexion permanente de la profession sur la sécurité des opérations.

En 2002, le niveau record des opérations effectuées par carte met fin à la primauté du chèque parmi les moyens de paiement. Par exemple, avec plus de 4,8 milliards d'opérations, le système "CB" devient le premier instrument de paiement dématérialisé en France.

Les entreprises bancaires françaises consacrent en moyenne cheque année plus de 150 millions d'euros au maintien et au renforcement de la sécurité des cartes bancaires.

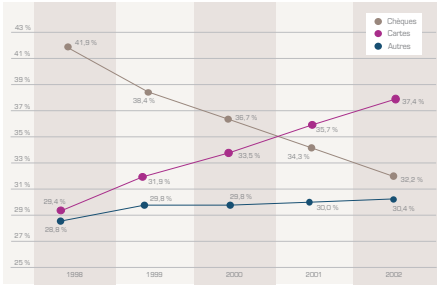
Depuis plusieurs années, elles ont entrepris un vaste programme pour moderniser l'ensemble de la chaîne monétique "CB", avec un double objectif :

- mettre en place un réseau d'autorisation plus flexible, mieux sécurisé pour les opérations par cartes bancaires "CB" ;
- adapter les cartes, terminaux de paiement et distributeurs automatiques à la nouvelle génération de puces renforçant le dispositif de sécurité.

En outre, la loi sur la sécurité quotidienne crée un Observatoire de la sécurité de toutes les cartes de paiement utilisées en France. Sa composition et ses compétences sont précisées dans un décret à la fin 2002. Un représentant de la FBF participe aux travaux de cet Observatoire qui a notamment pour mission "de proposer des moyens de lutter contre les atteintes d'ordre technologique à la sécurité des cartes de paiement".

POIDS RESPECTIF DES MOYENS DE PAIEMENT

En nombre de transactions réalisées au moyen de chèques, cartes ou autres (TIP, LCR)



Pour les cartes et les chèques, les transactions comprennent les paiements et les retraits
TIP : Titre Interbancaire de Paiement - LCR : Lettre de Change Relevé

SÉCURITÉ INTERNET

À l'issue d'un groupe de travail réunissant à la FBF banquiers et spécialistes de la sécurité, le Centre d'information bancaire a publié un mini-guide (Repère n°4) sur les bonnes pratiques à respecter en matière de sécurité des opérations sur Internet, tant au niveau des banques que des clients.

Les bonnes pratiques pour LA BANQUE

- **Faciliter l'accès et les opérations :** offrir dans toute la mesure du possible un accès 24 h/24 ; permettre d'obtenir en ligne le détail de toute opération affichée ; proposer un accusé de réception pour toutes les opérations exécutées sur ce canal ; demander confirmation avant enregistrement d'un ordre.
- **Assurer un haut niveau de sécurité :** sécuriser l'accès, au minimum par un identifiant et un mot de passe ; offrir la possibilité au client de modifier lui-même son mot de passe à tout moment ; donner la possibilité au client de bloquer son accès au service ; offrir un système de transmission sécurisé ; afficher la date et l'heure de la dernière connexion ; conseiller voire imposer l'utilisation d'une version du navigateur présentant un niveau de sécurité suffisant ; afficher sur tous les écrans un bouton permettant de quitter la banque en ligne ; déconnecter automatiquement en cas d'absence de transaction.
- **Informer sur les fonctions et les utilisations :** offrir une présentation en ligne des services de banque en ligne, indiquer les moyens et les conditions d'accès à un service d'assistance à la banque en ligne, présenter la politique de sécurité du site.
- **Présenter les recours possibles en cas de litige :** expliquer la marche à suivre, s'engager à rembourser après enquête toute opération imputée indûment au compte du client.

Les bonnes pratiques côté CLIENT

- **Protéger son code confidentiel :** le conserver en lieu sûr ; ne pas l'enregistrer automatiquement sur l'ordinateur ; ne pas l'inscrire en évidence ; ne le divulguer à personne ; en changer dès sa réception lors de la souscription au service ; par la suite, le changer régulièrement ; ne pas utiliser de code confidentiel facile à identifier.
- **Respecter les règles de prudence :** utiliser les boutons de déconnexion manuelle sitôt la consultation terminée plutôt que d'attendre la déconnexion automatique ; être particulièrement prudent pour tout usage d'un ordinateur en libre-service (voir nos conseils particuliers ci-après) ; utiliser un anti-virus régulièrement mis à jour ; prendre des mesures adaptées en cas de connexion permanente.
- **Informer la banque de toute anomalie :** signaler immédiatement à la banque la perte ou le vol des informations permettant d'accéder au service de banque en ligne ; contrôler régulièrement ses comptes ; signaler immédiatement toute anomalie à sa banque.
- **Prudence renforcée pour les utilisateurs d'ordinateur en libre-service,** susceptible de conserver des informations même après la fermeture de votre session.