Quelques recommandations pratiques

Lutter contre la fraude *nécessite de renforcer constamment les mesures en place et un engagement permanent de l'ensemble du personnel.*

OLIVIER JEREZ*
Docteur en droit
Caisse d'épargne Provence-Alpes-Corse-Réunion

LE BLANCHIMENT DES CAPITAUX est un nouveau risque pénal qui doit entrer aujourd'hui dans le cadre de la maîtrise du risque en général. Une meilleure organisation et gestion du risque bancaire s'impose. Les contre-mesures doivent être organisées notamment au sein du secteur opérationnel (réseaux commerciaux) et du secteur juridique.

UNE PRÉVENTION QUOTIDIENNE

L'appréciation en permanence des risques est une nécessité. Elle passe par la prise en compte de l'environnement sociétal et ses incidences sur la profession. Des fraudes (cartes bancaires, chèques, cyber-paiement, Internet, transferts de flux par le Monep-Matif, virements interbancaires…) interviennent davantage à certaines périodes. La spécificité de l'activité de certains établissements bancaires induit un risque propre, comme les banques d'affaires. Les données criminologiques sont donc nécessaires à la prévention, de même que la connaissance des mécanismes frauduleux.

« L'appréciation en permanence des risques est une nécessité. »

Outre la formation et la sensibilisation du personnel, la diffusion dans la banque des informations susceptibles d'impacter toutes les activités de l'entreprise (engagement, commercial, entreprise, maîtrise des risques, etc.) est primordiale. L'intranet devrait remplir mieux ce rôle. L'échange d'informations entre établissements bancaires concurrents, sans opposer systématiquement le secret bancaire, semble nécessaire. Il en va de la préservation des intérêts de tout le secteur bancaire.

Sur le plan dissuasif, il faut engager toutes les actions limitant les pertes financières de l'établissement et l'altération de sa crédibilité par la présence sur le terrain judiciaire. La lutte anti-blanchiment peut servir de base pour la construction d'un système préventif contre la fraude.

AMÉLIORER L'EFFICACITÉ DES SYSTÈMES MIS EN PLACE

Certains détecteurs (topages de comptes inactifs ou réactivés, opérations douteuses, supérieures à un montant fixé, transferts vers l'étranger ou pays *offshore*, etc.) doivent intervenir à certains moments de la vie du compte (création, ouverture d'un produit), mais aussi à l'occasion d'événements affectant le fonctionnement du compte (modification d'adresse, création de mandat, procuration, désolidarisation, perte/vol de chéquiers, cartes, etc.).

- Pour les opérations à distance, l'identification de la personne pose problème. Il n'est pas sûr que le client agisse pour lui-même : il faut donc exiger que le premier paiement de l'opération soit effectué par l'intermédiaire d'un compte établi dans un établissement de l'UE ou ayant les mêmes obligations antiblanchiment, et s'assurer de l'identité du client auprès de cet établissement ou qu'il atteste avoir effectué la vigilance

* Auteur de l'ouvrage «Le blanchiment de l'argent», *Banque éditeur*, 1998.

active. Ces mesures de renforcement sont d'ailleurs à l'ordre du jour de l'examen par le Parlement et le Conseil européen d'une modification de la directive du 10 juin 1991 relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux.

• L'expédition de la lettre d'accueil doit être automatisée tant lors de la l'ouverture d'un produit bancaire que lors de toute modification affectant le compte. Son retour NPAI à la banque doit parvenir au plus tôt à la cellule pour une action rapide, par exemple, blocage du compte jusqu'à régularisation.

• Lors de la constitution, gestion ou direction de société, fiducie ou de structures similaires, le contrôle doit être plus efficace.

• La loi du 12 juillet 1990 impose une déclaration de soupçon pour toute opération supérieure à 1 million de francs, «*se présentant dans des conditions inhabituelles de complexité ou sans justification économique licite*» avec l'activité apparente du client. La loi impose également un «*examen particulier*» (art. 14) par les banquiers. Ces règles de la «vigilence active» peuvent servir de vecteur à la prévention de la fraude en général. Ainsi, pour toute opération financière supérieure à 1 million de francs (prêt, souscription et remboursement de bons, contrat d'assurance vie, etc.), le responsable de la cellule interne sera informé de l'opération. C'est une alerte informative et informatique qui pourrait être calquée sur les «états» que gèrent déjà les agences commerciales (par exemple les chèques sans provision). Pour toute opération comprise entre 50 000 et 1 million de francs anonymes ou non, un examen pourra intervenir, non systématique, par le responsable d'agence. Un compte rendu d'opérations écrit sera adressé à la cellule.

• Chaque dépôt de plainte du client pour vol ou perte de chéquier ou carte bancaire, ou de la banque, doit impérativement venir nourrir une base de données que la cellule consultera. La cellule doit être la centralisation des lettres d'accueil, de toutes les réquisitions judiciaires ou de police, de même que les «avis à victimes» expédiés par les greffes des juridictions pénales.

• La gestion, après avis de la CNIL, d'un fichier interne où seraient recensés les clients «hors cibles», «indésirables» «à risque» (ayant fraudé ou tenté de frauder la banque), doit être assurée par la cellule. ■

« Chaque dépôt de plainte du client pour vol ou perte de chéquier ou de carte bancaire, doit impérativement venir nourrir une base de données. »

Les missions d'une cellule anti-fraude et blanchiment

Au même titre que la structure opérationnelle Tracfin, il faut créer une cellule opérationnelle interne composée d'un nombre limité de collaborateurs pour des raisons d'efficacité et de préservation du secret bancaire. Elle doit être un pôle interne de lutte anti-délinquance, et remplir les missions suivantes :

- rôle de sensibilisation et de formation **du personnel sur le risque pénal, quel qu'il soit ;**
- rôle d'interlocuteur privilégié des intervenants extérieurs **(Tracfin, autorités de police, judiciaires, parquets, etc.), mais interne également (réseau commercial Banque de France) ;**
- rôle de correspondant Tracfin : **chaque «correspondant Tracfin» devrait être connu par l'ensemble des banques pour un meilleur échange d'informations et une meilleure appréhension des risques ;**
- gestion des affaires de fraudes : **fichier des «clients douteux» ;**
- juger de l'opportunité des actions judiciaires : **déclaration de soupçon, application de l'article 40 du CPP, dépôt de plainte avec ou sans constitution de partie civile après une analyse in concreto du risque pénal ;**
- collecter, analyser **les remontées d'informations, «états» informatiques…**

Pour cela, la cellule doit être autonome, avoir une hiérarchie limitée, être l'interlocuteur de certaines structures internes (maîtrise des risques, inspection, audit, sécurité, engagement, etc.).
Il faut ensuite renforcer les systèmes de remontées d'informations vers cette cellule, par la mise en place de clignotants automatiques.
La cellule doit être en mesure, à un second niveau, de contrôler les informations qu'elle reçoit des directions opérationnelles, pour analyser in fine le risque bancaire.