Les établissements financiers touchés, eux aussi, par la fraude

VÉRONIQUE HACCOUN
Senior Manager, département Fraud Investigation & Dispute Services, Ernst & Young

TANGUY COATMELLEC
Associé, département Financial Services, Ernst & Young

L'évolution récente de l'industrie financière a été marquée par une internationalisation croissante des entreprises, une augmentation significative du volume des opérations traitées, un élargissement et une complexification de la nature des produits proposés. Cette complexité a souvent été le terreau de fraudes ou de manipulations comptables de grande envergure se traduisant, dans certains cas, par des scandales retentissants, voire par des faillites.

Si la règle veut que les fraudes bancaires soient rarement médiatisées, principalement en raison de la confidentialité inhérente à l'exercice même de la profession, l'industrie attache cependant une importance croissante au traitement des risques. Les régulateurs et les autorités de tutelle ont ainsi significativement renforcé l'arsenal réglementaire et législatif encadrant l'exercice du contrôle interne dans les établissements financiers et notamment le traitement de la fraude et du blanchiment d'argent. La décennie a également été marquée par l'alourdissement des sanctions financières acquittées par les établissements financiers à travers le monde.

Quel est le coût de la fraude ?

Selon l'*Association of Certified Fraud Examiners* (ACFE), la fraude représente pour les entreprises américaines une perte de 5 % du PNB soit, pour 2006, une somme de l'ordre de 652 milliards de dollars.

Avec 15 % de cas de fraude recensés et un coût moyen par schéma de fraude de l'ordre de 330 000 euros, le secteur bancaire semble être une cible de choix, d'autant qu'il faut en moyenne dix-huit mois pour détecter une malversation.

Les natures de fraude et le profil des fraudeurs

La nomenclature Bâle II distingue deux types de fraudes : internes et externes.

- Les malversation internes sont commises par ou en collusion avec des salariés pour une rétribution directe (partage du gain frauduleux avec un complice éventuel) ou une contrepartie plus indirecte (commissions sur la base de données financières fausses…). Elles prennent la forme d'activités non autorisées (transaction à pertes, intentionnellement non notifiée ou mal évaluée ou de détournements d'actifs).
- Les fraudes externes consistent, quant à elles, en des actes commis par des tiers au détriment de l'établissement bancaire : présentation de fausses informations pour obtenir un service indu ; détournement de fonds ou d'actifs, utilisation de circuits ou montages financiers impliquant la banque pour masquer l'origine frauduleuse des fonds.

Si ces fraudes concernent l'ensemble des métiers de la banque, ce sont les moyens de paiement qui cristallisent les principaux assauts avec, notamment, la falsification de chèques et de virements ainsi que les fraudes à la carte bancaire…

Les typologies de fraudes ne connaissent pas de limites et le raffinement des scénarios évolue au gré des contre-mesures mises en œuvre par les banques. Ainsi, malgré les dispositifs spécifiques de prévention et de détection renforcés après le 11 septembre, pour inclure notamment la lutte contre le financement du terrorisme, les schémas de fraude en matière de blanchiment se diversifient : dissimulation de fonds et usage détourné au sein d'activités ou de structures commerciales, utilisation de montages et d'instruments financiers toujours plus complexes ; usurpation d'identité, usage de faux, exploitation des différences de légis-

lations entre les juridictions de divers pays souverains ; recours à des formes d'actifs anonymes…

Le paradoxe est que, si la cellule française de lutte contre le blanchiment (TRACFIN) a vu plus que tripler le nombre des déclarations de soupçons qu'elle enregistre, cela traduirait dans certains cas plus un souci de couverture de la part des établissements financiers qu'une volonté d'analyse poussée des dossiers.

Les dispositifs de prévention

Le renforcement de la réglementation déjà évoqué, incluant notamment les recommandations du Comité de Bâle et le règlement CRBF 97-02 modifié en mars 2005, a eu pour conséquence d'accroître le devoir de vigilance et d'alourdir les sanctions associées. Cependant, ces réglementations, ambitieuses dans l'esprit, restent peu explicites sur la nature des dispositifs de prévention à mettre en œuvre. Et, dès lors que ces mêmes dispositifs ne sont pas spécifiques, ils restent peu efficaces.

Il n'existe pas de recette miracle pour prévenir et détecter à coup sûr la fraude, mais la prévention passe a minima par un contrôle interne efficace et un système d'information robuste.

Parmi les outils d'un tel dispositif, la charte d'éthique joue un rôle clé. Elle doit contenir un certain nombre de thèmes (conflits d'intérêts, confidentialité, comportements professionnels non acceptables, etc.), être disponible dans toutes les langues, mise à jour régulièrement et faire l'objet de formation régulière. Une attention particulière sera portée aux employés dits « sensibles » (trésoriers, gérants, *traders*, responsables de consolidation, acheteurs…) qui, par leur fonction et leur statut hiérarchique, peuvent abuser de leur savoir et/ou de leur pouvoir.

Par ailleurs, un strict suivi des opérations incompatibles, une mise à jour des délégations de pouvoir et des spécimens de signature, une information claire sur l'attitude à adopter en cas de suspicion de fraude (à qui communiquer, sous quel format) et des sanctions applicables en cas de fraude font partie intégrante des bonnes pratiques à mettre en œuvre.

> *« La fraude représente pour les entreprises américaines, une perte de 5 % du PNB soit, pour 2006, une somme de l'ordre de 652 milliards de dollars. »*

Le système d'information joue également un rôle essentiel, à la fois vecteur potentiel de fraude (utilisation du SI pour commettre la malversation) et moyen de détection des opérations malveillantes (existence d'états d'anomalies, analyse de données…). Il convient donc de déployer des dispositifs de prévention tout au long du cycle de vie d'une application.

Le traitement de la fraude

Lorsqu'une fraude est soupçonnée ou avérée, il faut gérer cela comme un contexte de crise à part entière, c'est-à-dire en mobilisant en urgence une équipe ad hoc dédiée à un projet sensible et confidentiel, qui sera en mesure de mener cette mission avec toutes les garanties de professionnalisme et d'indépendance nécessaires.

L'équipe qui diligente l'investigation doit être constituée de collaborateurs qui ont à la fois les compétences, l'expérience, l'autorité, la légitimité et la capacité à gérer leur mission dans un contexte difficile soumis à de fortes contraintes de délais et de pression.

En outre, certaines missions d'audit de fraude, si elles sont mal préparées, peuvent générer des risques pour l'établissement : perte ou disparition de preuves, impossibilité d'identifier les responsables et de prouver leur implication, actions en justice de la part des personnes mises en cause pour harcèlement ou diffamation… Il est donc impératif de décliner de manière extrêmement précise les étapes principales de l'investigation en faisant appel à des spécialistes en complément des équipes internes.

Des efforts à poursuivre

Une majorité de banques ont mis en place de nouveaux systèmes et processus pour surveiller les opérations sur la base d'outils de profilage, notamment dans le cadre de la lutte contre le blanchiment. Cependant, la plupart d'entre elles n'ont pas saisi cette occasion pour inclure également des contrôles contre la fraude, en particulier en identifiant et en pilotant, pour chaque risque significatif repéré, un dispositif adéquat.

La fraude est un risque à part entière avec un impact fort sur l'image des établissements bancaires qui en sont victimes. Les banques doivent donc poursuivre les efforts déjà entrepris en matière de prévention, analyser et capitaliser sur les cas de malversation passés.

Communiquer efficacement en interne et en externe, sur les dispositifs antifraude mis en place, constitue probablement un des outils majeurs de dissuasion contre les agissements frauduleux. ■

Enquête : « Dénoncer les abus liés à la fraude, aux pots-de-vin et à la corruption »

■ Selon une enquête du département « Fraud Investigation & Dispute Services » d'Ernst & Young, réalisée en mars dernier auprès de salariés européens, un quart des salariés français confirme l'existence de suspicions de fraude dans leur entreprise en 2006, contre 22 % en Europe occidentale.
D'ailleurs, 89 % des salariés français estiment que toutes les grandes sociétés devraient avoir un code de conduite, les deux tiers disposent d'un tel code.
Cependant, comparativement à d'autres pays européens, les Français n'apportent pas autant de crédit au code de conduite dans le cadre de la prévention et de la détection des fraudes, des pots-de-vin et de la corruption (55 % des Français contre 60 % en Europe de l'Est et centrale et 70 % en Europe de l'Ouest).
Enfin, seuls quatre interviewés sur dix (39 %) indiquent que les salariés de leur société se sentent libres de signaler un cas de fraude, de pot-de-vin ou de corruption suspectés. Un chiffre bien inférieur à la moyenne de l'Europe de l'Ouest (58 %).