La fraude comptable et financière aujourd'hui

À l'occasion d'une conférence organisée par l'Association des professionnels et directeurs comptabilité et gestion (APDC) qui œuvre pour la promotion de la fonction comptable en entreprise et dont un groupe de travail est dédié aux bonnes pratiques dans le domaine du contrôle interne financier, Jean-Marc Lefort, Associé Forensic, KPMG, a présenté un panorama de la fraude comptable et financière. Quel est le visage de la fraude en 2014 et comment lutter contre ?

QUE RECOUVRE LA FRAUDE COMPTABLE ET FINANCIÈRE ?

Définition

La fraude s'entend de l'acte intentionnel commis par une ou plusieurs personnes parmi les membres de la direction, les responsables de la gouvernance, les employés ou des tiers, impliquant le recours à des manœuvres trompeuses dans le but d'obtenir un avantage indu ou illégal.

REPÈRES

LE DÉLIT DE PRÉSENTATION DE COMPTES ANNUELS NE DONNANT PAS UNE IMAGE FIDÈLE DANS LES SOCIÉTÉS

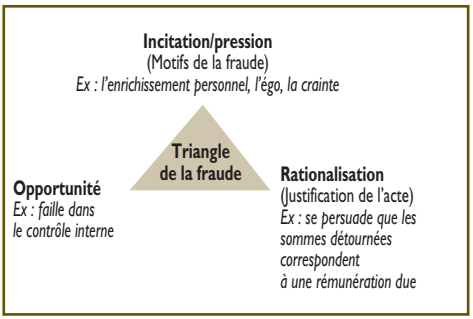
La présentation de comptes annuels ne donnant pas une image fidèle est pénalement sanctionnée dans les sociétés de capitaux dès lors que le gérant, le président, les administrateurs, les directeurs généraux, les membres du directoire, du conseil de surveillance, même en l'absence de toute distribution de dividendes, ont sciemment publié ou présenté aux associés des comptes annuels ne donnant pas une image fidèle du résultat des opérations de l'exercice, de la situation financière et du patrimoine à la clôture, en vue de dissimuler la véritable situation de la société (c. com. art. L. 241-3 ; L. 242-6, L. 242-30, L. 243-1, L. 244-1 et L. 246-2).

La fraude comptable et financière porte sur 3 domaines :

- *Le détournement d'actifs* (56 % des cas de fraude) : paiements frauduleux, vols, abus de biens sociaux, paiements de fournisseurs fictifs...
- *La corruption* (24 %) : conflit d'intérêt, délit d'initié...
- *La présentation frauduleuse des états financiers* (20 %) : comptabilisation de revenus fictifs, omission intentionnelle d'informations capitales, activation de coûts...

Le triangle de la fraude

Les éléments caractérisant la fraude peuvent être schématisés ainsi :



Le profil du fraudeur

Une étude de KPMG de novembre 2013 met en évidence les constats suivants (KPMG, « Global profiles of the fraudster », novembre 2013).

▶ 61 % des fraudeurs exercent dans l'entreprise victime, dont 41 % depuis plus de 6 ans.

▶ Dans 70 % des cas, le fraudeur est un homme entre 36 et 55 ans occupant un poste de manager.

▶ 54 % des fraudes sont commises par des employés ayant des fonctions d'encadrement ou de direction.

▶ La fraude excède 500 000 $ dans 32 % des cas.

▶ *Dans 70 % des cas,* le fraudeur agit en collusion avec d'autres individus et cette tendance est en constante augmentation.

Des exemples concrets

▶ *Situations à risque.* La vigilance est particulièrement de mise dans les situations, entités ou services suivants : périodes de vacances (absence du supérieur hiérarchique), services achats (frais généraux, travaux), phase de migration informatique, phase de réorganisation du service comptable, petite filiale géographiquement éloignée.

EXEMPLES

L'escroquerie au président – Elle consiste, pour le fraudeur, à contacter les services comptabilité ou trésorerie de la société cible en se faisant passer pour le président de cette même société ou de sa société mère en invoquant une opération très confidentielle en cours. Il va demander que soit réalisé en urgence un virement à destination d'un pays étranger.

La fraude aux virements SEPA – Profitant du contexte de migration (généralisation repoussée au 1er août 2014), le fraudeur s'improvise technicien de la banque de la société cible en prétextant des tests de compatibilité avec l'entreprise cliente pour demander à cette dernière de procéder à un paiement test.

La fraude aux coordonnées bancaires fournisseurs – Elle consiste à adresser au service comptable de la société un courrier sur papier en-tête d'un fournisseur pour l'informer d'un changement de RIB.

▶ *Les nouvelles technologies* ont, quant à elles, ouvert de nouvelles possibilités aux fraudeurs (la cybercriminalité).

CAS DE PIRATAGE INFORMATIQUE Mise hors service des systèmes, piratage du trafic réseau, scanning, social engineering, cracking des mots de passe, phishing.

LE DISPOSITIF – TYPE DE LUTTE CONTRE LA FRAUDE

Le point central de tout dispositif de fraude est la direction générale qui doit occuper un rôle central.

1) La prévention

▶ *La prévention passe en premier lieu par la désignation d'un responsable de la fraude*, un « fraud officer » qui joue un rôle d'animateur du processus de prévention.

« FRAUD OFFICER » VS RESPONSABLE DU CONTRÔLE INTERNE

Les mécanismes de fraude sont spécifiques et nécessitent la mise en place d'un contrôle interne spécifique, puisque la fraude suppose un acte volontaire, ainsi que des outils propres. Le « fraud officer » peut être le responsable du contrôle interne, mais il agira alors avec d'autres acteurs : l'auditeur interne, le security officer, la DSI, la DRH ou encore la direction juridique.

EXEMPLES

Des actions simples de prévention peuvent être mises en œuvre dans l'exemple de la fraude au président :
– sensibiliser l'ensemble des personnels des services « à risque » ;
– rappeler les procédures internes et l'interdiction d'y déroger ;
– réfléchir à la suppression des virements papier et renforcer les procédures de confirmation avec les banques ;
– revoir les firewalls informatiques protégeant le système de messagerie électronique ;
– limiter la diffusion de la signature du dirigeant sur Internet.

▶ *La cartographie des risques de fraude* est un autre élément important. La fraude est souvent intégrée dans la cartographie des risques, mais rarement comme un risque principal, il convient alors de cartographier spécifiquement le risque de fraude :
– identifier les risques majeurs,

– les décliner en risques spécifiques,
– convertir des risques bruts en risques résiduels (c'est-à-dire après prise en compte du contrôle interne),
– mesurer des risques résiduels sous deux dimensions (criticité et occurrence) et les hiérarchiser.

S'ensuivent des mesures correctives et un suivi.

2) La détection

Deux dispositifs méritent d'être soulignés.

Le whistleblowing ou l'alerte professionnelle – Ces dispositifs, autorisés par la CNIL depuis novembre 2005, sont relativement efficaces, mais impliquent la mise en place d'une organisation spécifique et un engagement de conformité aux conditions de la CNIL (CNIL, délibération, n° AU-004 modifiée par la délibération 14-042 du 30 janvier 2014).

L'alerte professionnelle s'adresse plutôt aux grands groupes et sociétés cotées ainsi qu'à leurs filiales.

Le data mining – Il s'agit d'une procédure d'extraction des données ERP pour être intégrées et traitées de façon périodiques par l'outil de data mining afin de générer des états d'exception à analyser. Ce sont de puissants outils nécessitant une maîtrise et de l'expérience pour affiner au maximum les résultats.

EXEMPLES

Les critères de recherche de données atypiques peuvent, par exemple, porter sur :
– des fournisseurs en doublon ;
– des fournisseurs français ayant un RIB dans une banque étrangère ;
– une écriture présentant un schéma atypique ;
– des comptes comptables rarement utilisés ;
– des sorties de stock annulées ;
– un utilisateur ayant saisi peu d'écritures ;
– des écritures comptabilisées sur une période normalement fermée.

3) L'investigation

Cette étape consiste à analyser des fraudes réelles et significatives via 4 techniques :
– l'audit classique ;
– le « forensic technology » (acquisition de documents électroniques afin de préserver les preuves) pour recueillir, parmi les données électroniques (mails, serveurs...) des éléments d'information sur des opérations potentiellement frauduleuses ;
– les entretiens avec les témoins ou les suspects ;
– le « corporate intelligence » (acquisition de données publiques relatives à des personnes physiques ou morales en lien avec des opérations potentiellement frauduleuses).

4) Les autres éléments du dispositif

Après l'étape de l'investigation, viennent celles :
– des actions correctives qui, suite à l'analyse des cas de fraude, permet d'identifier les faiblesses du contrôle interne et de définir les nouveaux contrôles ;
– du reporting et de la diffusion des retours d'expérience au sein du groupe ;
– de l'évaluation régulière du dispositif.

L'essentiel

- **La fraude n'est pas une simple erreur, elle suppose un acte intentionnel.**
- **Afin de lutter contre les manœuvres frauduleuses, les actions de communication au sein de l'entreprise sur la fraude sont essentielles.**
- **La direction générale a un rôle prépondérant dans tout dispositif anti-fraude.**
- **Le détournement d'actifs est le procédé le plus usité dans le cadre de la fraude comptable et financière.**
- **Retrouvez l'interview de Jean-Marc Lefort à la suite de cet article.**

Interview Jean-Marc Lefort, Associé Forensic, KPMG

La fraude comptable et financière en quelques chiffres

S'agissant par définition d'un phénomène occulte, les chiffres ne peuvent porter, par définition, que sur les fraudes découvertes et les statistiques chiffrées en la matière doivent toujours être considérées avec précaution.

Selon l'ACFE (Association of Certified Fraud Examiners), le coût des seules fraudes internes pourrait représenter en moyenne 5 % du chiffre d'affaires des entreprises. Autre chiffre édifiant : en matière de corruption, la Commission européenne avait évalué fin 2012 le coût de la seule corruption en Europe à 1 % du PIB, soit 120 milliards d'euros.

Y a-t-il plus de risques de fraude dans les petites entreprises que dans les grandes sociétés ?

Il n'existe pas, à ma connaissance, de statistiques précises en la matière. La distinction entre petites et grandes entreprises prête elle-même à discussion : un grand groupe peut être constitué de centaines de filiales, parfois de très petite taille. Ainsi, la seule distinction entre petites et grandes entreprises peut s'avérer non pertinente. En outre, les fraudes survenant dans les petites structures indépendantes sont moins répertoriées et donc moins étudiées.

Toutefois, on observe généralement que les défaillances de contrôle interne ayant favorisé les fraudes diffèrent selon les tailles des entreprises. Ainsi, dans certains cas, les éléments positifs en termes de prévention de fraude que l'on retrouve généralement dans les grandes sociétés (existence d'un contrôle interne fort, principe de séparation des tâches renforcé, etc.) sont parfois obérés par des dysfonctionnements également propres à leur taille (dilution des responsabilités managériales, inflation d'informations et de reportings non exploités, prépondérance de la « compliance » sur le contrôle effectif des opérations, etc.).

Selon vous, combien coûte la prévention de la fraude à une entreprise ?

L'un des freins à la mise en place d'un dispositif de prévention de fraude porte précisément sur la difficulté à en évaluer le coût. L'une des raisons de cette difficulté porte sur le champ d'application du contrôle interne qui va couvrir à la fois les risques d'erreur et de fraude. Dès lors, comment chiffrer le coût de la seule prévention de fraude ?

Plutôt qu'un chiffrage global, l'approche généralement retenue va consister à dresser une cartographie des risques de fraude et à rationaliser, dans la mesure du possible, pour chaque risque significatif, le rapport coût/avantage du dispositif de prévention envisagé. Pour chaque risque de fraude analysé, la méthode va consister à comparer le coût financier en cas de matérialisation du risque (pondéré par sa probabilité de survenance) avec les coûts de conception et de mise en place du contrôle visant à réduire ou supprimer le risque considéré.

Attention toutefois aux arbitrages strictement financiers qui pourraient conduire l'entreprise à ne pas couvrir un risque de fraude et ne négligeons pas les effets potentiellement dévastateurs d'une fraude de grande ampleur pour un groupe, notamment en termes d'image.