Fraudes et escroqueries au paiement en entreprise et cybercriminalité

Description, mécanismes, prévention, réparation

8 juin 2016

Sylvie Sanchis, Commissaire de police
Christian Connor, associé, Lmt Avocats
Jérôme Rousselle, collaborateur senior, Lmt Avocats

Lmt Avocats

1. Constat et état des lieux

1.1. **Variété des entreprises concernées**

- De grandes entreprises
- Des PME importantes
- Des petites entreprises

Aucune entreprise n'est épargnée par le risque
Les grandes entreprises s'estiment protégées
Les petites entreprises ne s'estiment pas concernées

1.2. Les **entreprises françaises** particulièrement ciblées

1. Constat et état des lieux

1.3. **Importance** de la fraude : chiffres et statistiques

Etude Euler Hermes 2016

- **93 %** des entreprises ont déjà subi au moins une tentative de fraude (77 % en 2015)
- **20 %** ont subi plus de 10 tentatives de fraude (17 % en 2015).
- **55 %** des victimes ont été visées par une fraude au président
- Estimation du préjudice des dernières années : **500 millions d'euros en France – 2,3 milliards de dollars entre 2013 et 2016 au plan mondial (FBI)**
- **900 millions d'euros de tentatives**
- **1550** entreprises victimes(selon l'office central pour la répression de la grande délinquance financière)

1. Constat et état des lieux

- Les escrocs tirent profit de l'ignorance par les victimes de leurs modes opératoires

- Connaissance et sensibilisation des personnes concernées réduisent considérablement le risque et constituent une première assurance: 27 % des entreprises connaissent les typologies de fraudes

2. Qualification juridique et jurisprudence au pénal

- Escroquerie: Code pénal article 313-1
- Faux : Code pénal article 441-1
- Intrusion dans un système de traitement de données : Code pénal articles 323-1 et suivants

- Très peu de décisions car les modes opératoires des escrocs, situés le plus souvent à l'étranger, ne permettent en fait que peu de poursuites.

- Jugement du Tribunal correctionnel de Paris du 20 mai 2015: 7 ans d'emprisonnement et un million d'euros d'amende pour des escroqueries au préjudice de plusieurs banques et entreprises. 5,5 millions d'euros de dommages et intérêts au profit de plusieurs victimes.

2. Qualification juridique et jurisprudence au civil

- Faute caractérisée par un manquement de la banque à son devoir de vigilance

La jurisprudence civile retient la responsabilité de la banque lorsqu'un manquement à son devoir de vigilance est constaté (Cass.com., 22 novembre 2011):

- absence de pouvoir du donneur d'ordre
- absence de vérification de la signature
- circonstances inhabituelles au regard du fonctionnement du compte: opération, bénéficiaire du virement
- procédure de contrôle insuffisante: contre-appel non effectué ou mal dirigé

2. Qualification juridique et jurisprudence au civil

Dans la très grande majorité des cas, la banque sera condamnée à rembourser l'intégralité des fonds, un partage de responsabilité avec l'entreprise pouvant être prononcé.

- Tribunal de commerce de Paris, 30 octobre 2014; Cour d'appel de Paris, pôle 5 chambre 6 18 décembre 2014; Tribunal de grande instance de Montpellier 12 mars 2008 : banque condamnée à rembourser intégralement

- Cour d'appel de Bordeaux chambre 2, 17 avril 2015: partage de responsabilité entre la banque et le client

3. Connaître les fraudes pour les prévenir

3.1. Présentation des principales fraudes et modes opératoires

Selon une étude récente *(« Baromètre Sage 2016 des Directeurs Financiers : sécurité des virements et prévention des fraudes »)* :

- **83 %** des entreprises ayant déjoué une tentative de fraude y sont parvenues grâce à la vigilance des collaborateurs
- **66 %** grâce au respect des procédures de contrôle interne

Connaître les principales fraudes constitue le premier stade de protection et le préalable à toute formation pour les prévenir

3. Cybercriminalité

- Affaire BeIN Sports / HSBC: jugement du tribunal de commerce de Paris du 9 mars 2015

Un exemple de modes opératoires croisés

3. La fraude au président

La phase de préparation

Les fraudeurs mènent l'enquête : Précision, Anonymat, Sophistication

La phase opérationnelle

Les fraudeurs en action: Intimidation, Conviction, Manipulation

Recours à des fausses qualités internes (Président) et externes (avocat, expert comptable, agent secret)

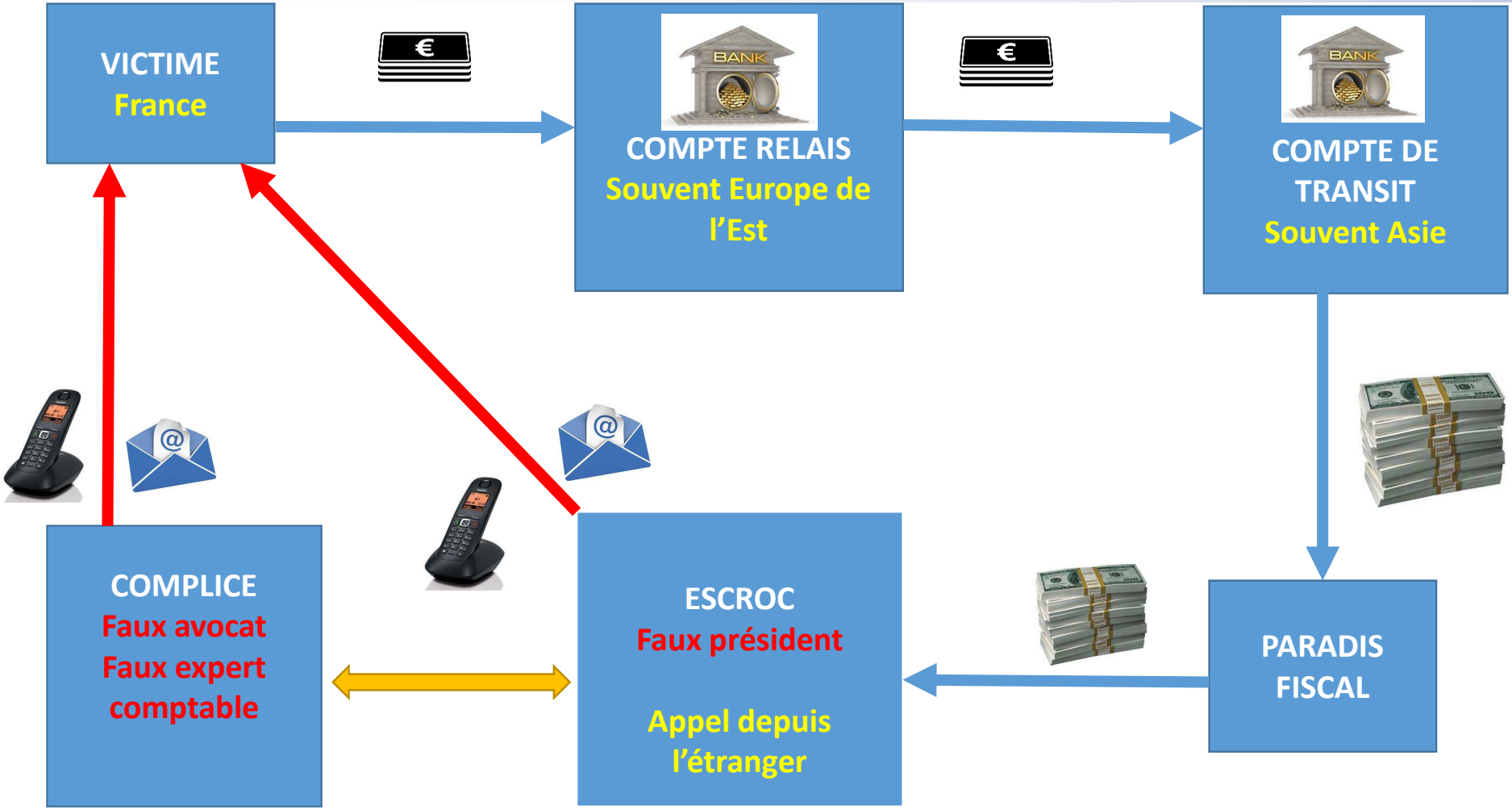
3. La fraude au président

Le résultat

Les fonds sont virés sur des comptes « relais » ou « rebond » (souvent Europe de l'Est) puis les fonds transitent le plus souvent par la Chine avant d'être redirigés.

Objectif: rendre le gel des avoirs difficile lorsque la victime découvre la fraude.

3. La fraude au Président



3. Connaître les fraudes

Points communs aux types de fraude : l'ingénierie sociale et outils informatiques : recherche et collecte de données les plus précises possibles sur l'entreprise ciblée et ses collaborateurs sur tous les vecteurs d'informations disponibles.

3. Connaître les fraudes

- **Captation d'informations :**
  - ⟹ sur les réseaux sociaux
  - ⟹ sur les sources officielles (infogreffe)
  - ⟹ sur les documents de l'entreprise (plaquette commerciale : logo etc).
  - ⟹ vol de courriers (factures, coordonnées bancaires, fichier clients)
- **Utilisation des outils informatiques** : Faux mails, fausses adresses, numéro apparemment local mais en réalité sur une plateforme délocalisée, mail phishing, logiciel espions, adresse IP.

3. Prévenir les fraudes

3.3. Trois axes :

- Former les collaborateurs de l'entreprise
- Mettre en place des procédures internes
- Sécuriser la relation avec la banque

3. Prévenir les fraudes

3.4. Sensibiliser et former les collaborateurs de l'entreprise:

- **A repérer** une demande inhabituelle : virement urgent, confidentiel, à destination d'un pays étranger sans rapport avec l'activité habituelle de l'entreprise, montant inhabituel, moment choisi
- **A détecter** un changement inhabituel de procédure : une demande d'ordre de virement par fax à la banque au lieu d'un ordre dématérialisé est le signe d'une volonté de contourner la sécurité des paiements, un changement soudain de RIB d'un fournisseur ou bailleur
- **A se méfier** de tout changement de coordonnées téléphoniques ou de mails de l'interlocuteur (dirigeant ou fournisseur) : attention, un numéro d'appel avec indicatif français n'est pas une garantie
- **A prendre** le temps de la vérification : contre appel, vérification de factures antérieures, consultation de la hiérarchie
- **A identifier** une mise en condition pour ne pas y entrer (flatterie, menaces, ton inhabituel, fournitures d'informations confidentielles) et l'intervention d'un tiers complice
- **A ne pas s'isoler**: communiquer ses doutes à un référent, valider l'opération demandée par email interne pour déjouer le caractère secret et confidentiel demandé par l'escroc

3. Prévenir les fraudes

3.4. Sensibiliser et former les collaborateurs de l'entreprise:

- **Identifier les collaborateurs exposés :** comptabilité, trésorerie, secrétariat, standard et les sensibiliser au risque de fraude en leur présentant les modes opératoires et les signes d'alerte
- **Former régulièrement**: ne pas omettre les remplaçants sur ces postes. Répéter les consignes à intervalles régulier et assurer les collaborateurs qu'ils ne seront pas sanctionnés pour un excès de méfiance
- **Attirer l'attention** sur la vigilance dans les périodes de vacances scolaires, de congés, les veilles de week end prolongé ou de pont.
- **Faire signaler** à la hiérarchie toute suspicion ou tentative: un vol soudain de courriers: signes de collecte en amont d'informations, tentative de contacts même repoussée (récidive fréquente vers un autre collaborateur)
- **Auditer** les failles avec un Conseil : état des lieux, stress test, consignes et procédure interne

3. Prévenir les fraudes

3.5. Mettre en place une procédure interne

- **Identifier** les personnes habilitées à effectuer des virements
- **Prévoir** une double signature, un montant plafonné,
- **Respecter** les modes de paiement sécurisé (EBICS TS signature électronique par clé) et ne pas y déroger
- **Séparer** les tâches pour compliquer la tâche des escrocs. L'ordonnateur du virement n'est pas celui qui l'effectue
- **Sécuriser** l'accès aux services bancaires en ligne et les installations informatiques : mail phishing, logiciel espion
- **Exiger** la confirmation de toute opération suspecte: auprès du dirigeant ou d'un référent

3. Prévenir les fraudes

3.6. Sécuriser la relation avec la banque

Deux objectifs: Empêcher la fraude ou caractériser une faute de la banque si la fraude aboutit

- **Mettre en place** un mode de paiement sécurisé (EBICS TS signature électronique par clé)
- **Prohiber** expressément l'usage d'autres modes: fax, téléphone
- **Prévoir** des listes blanches de bénéficiaires approuvés (SEPA)
- **Convenir** d'une procédure de gel du virement jusqu'à vérification: contre appel, SMS et email au dirigeant ainsi qu'à une autre personne désignée

3. Prévenir les fraudes

3.7. Sécuriser la relation avec la banque

Les principales fraudes concernent les virements par fax. En 10 ans, aucune tentative de fraude externe n'a été recensée pour les opérations sur support EBICS T et TS qui vont devenir la norme.

 Si l'entreprise effectue ses virements sous format électronique, les escrocs chercheront à contourner le système en obtenant un ordre par fax par la manipulation d'un collaborateur de l'entreprise.

4. Quelle réaction adopter en cas de constat d'une fraude réussie ?

1. **Alerter** sans attendre la banque : objectif de geler les fonds si possible (48 heures maximum) et obtenir un retour ou à défaut des éléments de preuve
2. **Contacter** aussitôt son conseil pour mettre en place les actions à mener
3. **Retracer** au plus vite le scénario de la fraude avec la collaboration du membre de l'entreprise trompé par les escrocs : conservation des emails, fax, ordres de virement, description des appels téléphoniques
4. **Assurer** le membre de l'entreprise du soutien de sa hiérarchie
5. **Constituer** avec son Conseil un dossier complet en vue de déclarer un sinistre à l'assurance ou de rechercher la responsabilité de la banque

4. Agir et réparer la fraude

4.1. La voie pénale

- **Contacter** aussitôt son Conseil pour mettre en place les actions à mener et déposer plainte
- **Alerter** sans attendre les services de police: obtenir une meilleure collaboration de la banque et des éléments de preuve via la procédure pénale
- **Retracer** au plus vite le scénario de la fraude pour communication aux services de police

4. Agir et réparer la fraude

4.2. La voie civile

- **Vérifier** si le collaborateur s'est conformé aux procédures internes et formations reçues pour identifier une éventuelle faute interne

- **Constituer** avec son Conseil un dossier complet afin de caractériser un éventuel manquement de la banque à son obligation de vigilance: respect par la banque des procédures mises en place

- **Contacter** la banque aux fins d'indemnisation:

➢ annulation du virement et récupération des fonds
➢ assignation de la banque pour manquement au devoir de vigilance
➢ transaction avec la banque

4. Agir et réparer la fraude

4.3. L'assurance

Ceci suppose d'avoir souscrit antérieurement aux faits un contrat d'assurance spécifique couvrant les risques particulier liés aux actes délictueux.

Face à la fréquence et à l'ampleur des fraudes au virement, plusieurs compagnies d'assurance proposent des garanties spéciales.

- **Constituer** un dossier et déclarer le sinistre à l'assurance

4. Agir et réparer la fraude

Les contrats d'assurance proposés peuvent couvrir:

- la fraude interne: commise par un collaborateur
- La fraude externe : commise par un tiers (parfois avec la complicité d'un collaborateur)
- La cyberfraude

Ils peuvent prévoir:

- **une indemnisation** (intégrale ou partielle) du préjudice pour limiter les pertes financières
- **une prise en charge** d'une partie des frais de communication pour la restauration de l'image de l'entreprise
- **une prise en charge** des frais de reconstitution des données et de restauration de la capacité du réseau en cas de cyberattaque

Merci de votre attention

Sylvie Sanchis, Commissaire de police
Christian Connor, associé, Lmt Avocats
Jérôme Rousselle, collaborateur senior, Lmt Avocats

www.lmtavocats.com