L'influence positive de **la lutte contre la fraude**

LIVRE BLANC

Édito

Jean-Baptiste AUZOU

DIRECTEUR GÉNÉRAL

ACA *Expert en gestion de flux & processus de gestion*

La fraude est un sujet d'inquiétude, d'interrogation pour l'ensemble des acteurs économiques. Nous réalisons un focus, à travers ce livre blanc, sur la fraude aux moyens de paiements.

En effet, la fraude aux identités bancaires, les faux ordres de virement, la fraude à la carte bancaire et la médiatique fraude au président semblent exploser en France et en Europe.

Des facteurs sociétaux viennent aggraver la situation, la crise économique, les difficultés de certaines régions du globe, l'instabilité politique de certains pays poussent des individus et des groupes à frauder. En complément et en support, la technologie de plus en plus répandue et accessible permet la réalisation de fraudes extrêmement sophistiquées !

Aujourd'hui, tous les acteurs économiques peuvent être touchés par les tentatives d'escroqueries, petites entreprises ou groupes internationaux, sociétés aux capitaux privés ou groupes côtés sur les marchés mondiaux, personne n'est au-dessus ni à l'abri du risque.

Les résultats de ces fraudes peuvent être catastrophiques pour les entreprises et aller jusqu'à la disparition de PME et nous ne pouvons que confirmer et réaffirmer les règles de base de lutte contre la fraude, comme mettre en place et respecter une procédure pour le traitement des virements en lien avec la banque, réduire au maximum le partage d'informations sensibles sur l'organisation, mettre en place une sécurité informatique forte et sécuriser les accès à distance des banques.

Mais les résultats sont parfois bien pires pour les femmes et les hommes victimes de ces fraudes. Briser l'isolement des individus victimes de ces fraudes est majeur et sensibiliser, informer, former ses collaborateurs sur les différents risques. Organiser des procédures d'alerte est primordial dans la démarche.

Cependant, trop souvent, la lutte contre la fraude se limite à traiter des aspects techniques ou au mieux organisationnels. Nous souhaitons aborder à travers ce livre blanc, et au-delà des outils, des méthodologies et des solutions, une approche positive de cette lutte.

Nos experts, nos partenaires expliquent comment transformer cette lutte, comment passer de ces cas de fraudes volontairement cachés, occultés par peur, par honte, par isolement à une utilisation interne à l'entreprise et externe vis-à-vis du marché, à un usage positif de cette fraude ou de cette lutte contre la fraude. Nous pouvons aller jusqu'à mettre en œuvre un côté enchanteur à cette lutte.

C'est-à-dire comment utiliser, au sein d'une organisation, la lutte contre la fraude comme un véritable moteur interne :

> Un enjeu sur l'explication de cette lutte,

> Un enjeu de communication interne auprès de l'ensemble des Collaborateurs,

> Un enjeu de rassurance des clients, des partenaires économiques et financiers, du marché quant à ses méthodes.

À partir d'un constat de l'état d'avancement des organisations sur la lutte contre la fraude dressé par Grant Thornton et son panorama annuel de la fraude, nous aborderons, ce qui est assez rare pour être mis en valeur et nous les en remercions, deux cas de fraudes vécus et les procédures mises en place sans oublier de remettre l'humain au cœur du dispositif.

Intervenants

ACA REMERCIE L'ENSEMBLE DES PARTICIPANTS À CE LIVRE BLANC !

Jean-Baptiste AUZOU
Directeur Général d'**ACA**

Patricia POMBO
Manager en charge de l'offre fraude au sein du cabinet Grant Thornton

Valérie DURAND-FANTUZZI
Responsable Dpt Trésorerie, Moyens de Paiements & Assurances PMU

Pierre-Yves HENTZEN
Directeur Administratif & Financier/CFO de la société Stormshield et président DFCG Rhône-Alpes Auvergne

Isabelle CATUSSE
Vice-présidente de la Commission Fraude AFTE et Responsable Trésorerie Groupe Guerbet

François LECOMTE-VAGNIEZ
Associé Lobary (www.lobary.com)

Sommaire

01 LE PANORAMA DE LA **FRAUDE**

Grant Thornton a réalisé un baromètre fraude en 2015 auprès de plus de 3000 entreprises et il en ressort que la fraude **n'est pas un risque théorique.** En effet, **77 % des entreprises ont déjà subi un cas de fraude.**

Pour autant, beaucoup d'entreprises ne se sentent toujours pas concernées ou exposées au risque de fraude alors que nos expériences permettent d'affirmer que :

> **Tous les secteurs d'activité** sont exposés à la fraude

> Les fraudeurs s'attaquent aujourd'hui à **toutes les tailles d'entreprises** (TPE – PME et grandes entreprises).

De même, si la probabilité de survenance du risque de fraude peut paraître faible il faut être conscient des conséquences lourdes que peut engendrer la survenance d'une fraude pour l'entreprise :

> Des conséquences financières : La perte médiane annuelle occasionnée par la fraude représente 5% du chiffre d'affaires d'une entreprise. Associée à la durée médiane d'une fraude à savoir 18 mois, il est clairement établi que la fraude peut mettre à mal une entreprise.

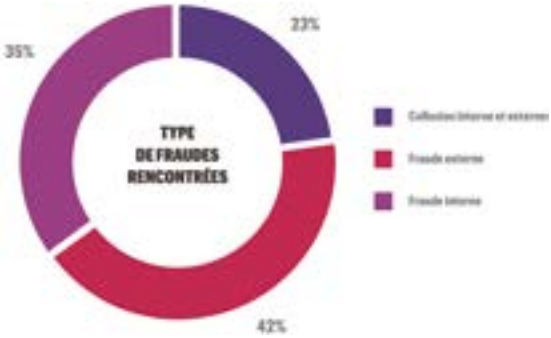
> Des conséquences en termes de réputation : Mise en avant des failles de l'entreprise auprès de l'ensemble de ses parties prenantes (clients – partenaires commerciaux – tutelles – salariés – actionnaires...).

> Des conséquences légales : Mise en cause de la responsabilité juridique du dirigeant pour faute de gestion.

D'où l'importance des dispositifs préventifs qui permettent non seulement de **limiter le passage à l'acte** mais également de **réduire la durée de la fraude** et donc **ses impacts financiers et organisationnels.**

Si les entreprises sont plus ouvertes au traitement du risque de fraude externe, il ne faut pas omettre la fraude interne qui peut être très dévastatrice pour l'entreprise.

En effet, l'étude démontre que dans presque **60 % des cas de fraude rencontrés un collaborateur de l'entreprise est impliqué.**



Les conséquences d'une fraude interne p**euvent avoir des impacts plus lourds pour l'entreprise que lors d'une fraude externe** du fait que :

> **La détection** de la fraude interne est souvent rendue difficile par la très bonne connaissance de l'organisation qu'a le fraudeur, lui permettant ainsi de camoufler au mieux ses opérations illégales ;

> **Le profil type du fraudeur interne** est généralement une personne sympathique, appréciée par ses collègues, disponible, agréable et qui n'éveille donc pas les soupçons ;

> **La fraude** peut être **commise par des dirigeants** il est compliqué de la détecter car les processus de contrôles sont souvent différents et non systématiques (exemple : contrôle des dépenses...)
La fraude a donc la capacité de durer plus longtemps et peut venir détériorer le climat social et la confiance entre les salariés.

POINTS À RETENIR

> **Le risque de fraude n'est pas un risque THÉORIQUE.**
> **Ce ne doit pas être un sujet TABOU au sein de l'entreprise.**
> **Le dispositif de lutte contre la fraude doit porter aussi bien sur la fraude interne que la fraude externe.**

Lorsque l'on demande aux entreprises leur préoccupation en matière de risque de fraude, la cybercriminalité ressort en premier. Ce point s'explique notamment par le fait qu'il s'agit d'un sujet d'actualité.

Toutefois, les risques de fraude classiques tels que :

- la falsification comptable et financière,
- le détournement d'actifs & l'escroquerie restent dans les préoccupations premières des entreprises.

Ainsi et au regard de ces typologies, il est important que l'entreprise ait connaissance des scénarii de risques auxquels elle est exposée.

Enfin, l'arrivée de la loi Sapin II va obliger des entreprises (500 salariés & 100 millions d'euro de Chiffre d'Affaires) à plus se préoccuper du risque de corruption qui ne ressort pas des préoccupations actuelles et qui est plus difficile à adresser que le risque de fraude.

POINTS À RETENIR

- **Donner une définition claire de la fraude.**
- **Définir l'univers de risques de fraude de l'entreprise.**

Si la fraude ressort comme une préoccupation pour les entreprises, **la mise en place d'une organisation dédiée n'est pas toujours une réalité.**

Ce constat s'explique généralement par deux raisons principales :

- L'entreprise n'est **pas consciente** de son **intérêt** et de son **retour sur investissement** :

  Hormis la quantification des scénarii de fraude de l'entreprise qui permettent d'avoir une idée des pertes financières potentielles en cas de fraude, il est difficile de donner un chiffre précis en matière de ROI car le retour sur investissement est qu'il ne se passe ... rien !

- Les sujets sont portés par les **équipes contrôle interne, gestion des risques** et **audit interne** déjà en place.

Il est important que l'entreprise ait conscience que la fraude est un risque spécifique qui demande systématiquement un ajustement des dis- positifs de contrôle interne déjà existants.

Ainsi, la pertinence de l'organisation à mettre en place doit être **examinée au regard des enjeux spécifiques de l'entreprise :** par exemple du data analytics sera très pertinent pour les activités décentralisées, les auditeurs internes formés au risque de fraude est nécessaire pour auditer les activités ayant des flux financiers importants, ou pour mener des investigations en cas de soupçons de fraude...)

POINTS À RETENIR

- **Etre conscient que la gestion du risque de fraude demande des compétences spécifiques au niveau des activités de gestion et maîtrise des risques (Contrôle & Audit interne)**

- **Adapter en permanence son dispositif de contrôle interne notamment pour les entreprises en forte croissance qui sont plus vulnérables du fait de règles organisationnelles et d'une culture de gestion du risque de fraude « artisanales »**

AU REGARD DE CES CONSTATS, QUEL DISPOSITIF DÉPLOYER AU SEIN DE SON ENTREPRISE POUR PRÉVENIR ET LUTTER CONTRE LA FRAUDE ?

LES 3 VOLETS CLÉS D'UN **DISPOSITIF DE LUTTE CONTRE LA FRAUDE...**

La mise en œuvre d'un dispositif de lutte contre la fraude efficace implique de développer trois volets **complémentaires qui participent à la fois à la performance de l'entreprise et à son image auprès de l'ensemble de ses parties prenantes :**

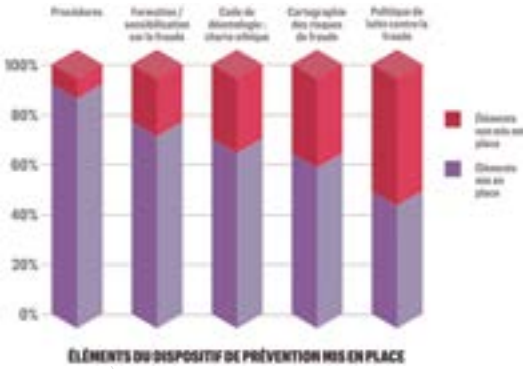
Si les 3 volets ressortent comme complémentaires, nous constatons que les entreprises sont plus attachées au **développement de la prévention qui reste bien évidement l'élément central d'un dispositif de lutte contre la fraude performant**. Toutefois, l'entreprise doit être consciente que le volet prévention ne se suffira pas à lui- même et nécessitera forcément un volet détection pour venir appuyer les principes généraux de la politique de lutte contre la fraude et maîtriser les zones de risques.

Volet prévention

Le volet prévention constitue la **pierre angulaire du dispositif de lutte contre la fraude** et doit permettre de calibrer les deux autres volets.

Toutefois notre expérience, appuyée par les résultats de l'enquête, révèle que les entreprises construisent leur dispositif de prévention à l'envers.

En effet, plus de 80% d'entre elles disposent de procédures alors qu'à peine, 50 % disposent d'une politique de lutte contre la fraude, 63% d'une cartographie des risques de fraude et 65 % d'un code éthique.



ÉLÉMENTS DU DISPOSITIF DE PRÉVENTION MIS EN PLACE

Ces chiffres viennent appuyer ce que nous pouvons constater lors de nos interventions :

Les entreprises ayant des procédures sans une « approche risque » en amont disposent de procédures génériques souvent inadaptées aux scénarii de risques de fraude auxquels l'entreprise est réellement exposée.

Il est donc essentiel que l'entreprise développe un volet prévention structuré autour des points suivants :

GOUVERNANCE :

> Fixer les ambitions de la gouvernance > Définir les enjeux et objectifs de son dispositif de lutte contre la fraude

APPROCHE RISQUE :

> Définir le profil de risque à l'aide d'une cartographie des risques de fraude
> Le cas échéant, quantifier les risques pour connaître les enjeux et décider des actions et investissements à mettre en œuvre

PROCÉDURES :

> Traduire de manière opérationnelle les processus & contrôles qui doivent être mis en œuvre pour réduire le niveau d'exposition de l'entreprise au risque de fraude

SENSIBILISATION :

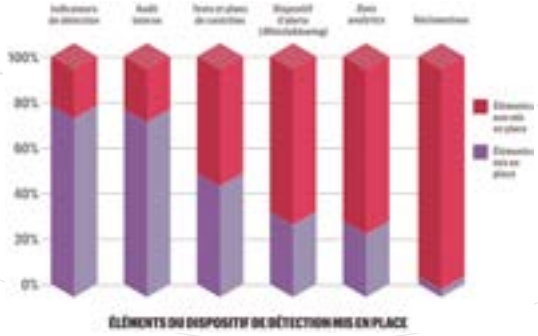
> Démontrer aux collaborateurs qu'il s'agit d'un réel sujet de préoccupation pour l'entreprise
> Rappeler l'existence et l'articulation du dispositif de contrôle interne et dissuader les éventuels fraudeurs
> Communiquer sur l'efficacité du dispositif

Volet détection

Ce volet consiste à définir les processus et contrôles qui permettrons à l'entreprise de détecter des opérations atypiques et en lien avec les scénarii de risques de fraude identifiés.

Nous constatons que les mises en place d'indicateurs de détection et d'audit interne ressortent clairement comme des pratiques dominantes et bien installées dans la plupart des entreprises.

En revanche, les déploiements de plans de tests et d'outils de data analytics restent minoritaires alors qu'ils constituent, de par notre expérience, la clé de voûte de l'efficacité des systèmes de détection, en permettant des approches systématiques, voire prédictives.



ÉLÉMENTS DU DISPOSITIF DE DÉTECTION MIS EN PLACE

Enfin, il est important que les salariés ne se sentent pas isolés en cas de soupçons de fraude et c'est pourquoi la mise en place d'un dispositif de remontée des alertes est importante.

Toutefois, l'enquête révèle la faiblesse du niveau de mise en place d'un dispositif d'alerte (whistleblowing – réclamation) que l'on peut expliquer par des freins d'ordre culturel ou social et que son efficacité au sein des entreprises l'ayant déployé n'est pas toujours démontrée.

Volet Protection

Un volet protection complet s'articule autour de deux axes :

- **Un axe forensic** pour traiter les cas de fraudes avérées dans toutes leurs dimensions :

  Investigations > Disposer d'une méthodologie d'investigation et d'experts (internes ou externes) garantissant la collecte des éléments probants qui pourront être présentés en cas de fraude avérée

  Gestion de crise > Avoir formalisé son dispositif de gestion de crise à activer en cas de soupçon ou de révélation publique de fraude (composition de la cellule de crise, actions clés à mener, les partenaires clés identifiés, les sanctions à appliquer...)

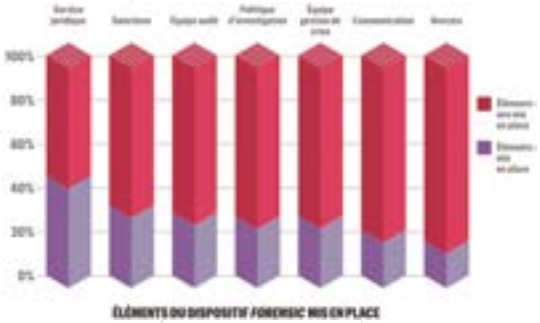
- **Un axe protection financière** pour se prémunir des conséquences économiques de la fraude :

  Assurance > Élément permettant de diminuer les impacts financiers d'une fraude.

D'après notre baromètre une entreprise sur deux ayant évalué le coût de la fraude a souscrit à une police d'assurance. Ce point s'explique par le fait que la quantification des risques permet de challenger l'intérêt d'une assurance.

Toutefois, nous constatons que ce volet protection est celui le moins déployé au sein des entreprises et peut s'expliquer par :

L'absence de cas avérés pouvant pousser l'entreprise à développer ce volet ;
Un besoin d'expertises spécifiques (investigations – juridique) ;
Une méconnaissance des solutions assurantielles.



ÉLÉMENTS DU DISPOSITIF FORENSIC MIS EN PLACE

Nous constatons également que la mise en œuvre de sanctions ainsi que leur communication au sein de l'entreprise ne sont pas des outils suffisamment développés alors qu'elles constituent un bon outil dissuasif en cas de fraude interne notamment. En effet, seul un tiers des entreprises ayant subi une fraude déclare mettre en œuvre des sanctions.

Nous constatons que trop souvent encore, il n'existe pas d'organisation structurée au sein des entreprises pour faire face efficacement au risque de fraude.
Il est de ce fait essentiel d'arrêter une véritable feuille de route, adaptée aux ambitions, ressources et contraintes de chaque entreprise, qui permette de développer progressivement un dispositif complet couvrant à la fois les dimensions prévention, détection et protection.

Conclusion

La gestion du risque de fraude ne doit donc pas être négligée par les entreprises notamment au regard des impacts que sa survenance peut engendrer et doit être conscient des bénéfices que peut apporter la mise en place d'un dispositif de prévention et de lutte contre la fraude :

- Assurer la pérennité de l'entreprise en protégeant sa trésorerie : on constate un grand nombre de faillites de petites entreprises dues à une ou plusieurs fraudes ;

- Prendre conscience de ses actifs et de leur valeur pour mieux les protéger ;

- Développer les engagements de l'entreprise en termes d'éthique et de transparence qui sont des notions de plus en plus exigées dans les relations d'affaires ;

- Redonner du sens aux fondamentaux du contrôles interne et actualiser les principes de contrôles internes de l'entreprise au regard des spécificités du risque de fraude ;

- Savoir agir en cas de crise (nécessité d'adapter son dispositif de crise aux cas de fraudes)

- Préserver la responsabilité juridique de la personne morale mais également du dirigeant qui peut-être mis en cause pour faute de gestion.

Patricia POMBO
Manager en charge de l'offre fraude au sein du cabinet Grant Thornton

02 RETOUR D'EXPÉRIENCE : **TÉMOIGNAGE DU PMU**

Fraude : quelles procédures sont mises en place

Le PMU a fait face à sa première fraude importante de type fraude à la carte bancaire en 2011 avant la mise en place de la 3D Secure. Victime d'une véritable bande organisée, les fraudeurs ont misé sur le manque de connaissance de la société face à une situation de fraude.

Force est de constater que depuis 5 ans les tentatives de fraudes ont considérablement augmenté obligeant les entre- prises à renforcer leurs règles et bonnes pratiques.

«Au sein du PMU nous ne parlons d'ailleurs pas de procédures mais plutôt de l'usage de bonnes pratiques au quotidien ».

Les fraudeurs sont aujourd'hui extrêmement bien renseignés. Lors de la dernière tentative déjouée, les fraudeurs ont appelé sur un numéro de portable professionnel et connaissaient le nom du PDG et du directeur financier.

Le maître-mot aujourd'hui au PMU est « tout ce qui sort des process habituels n'est pas normal ». C'est une consigne simple et efficace. Les équipes ont donc pour instruction en cas de situation anormale d'en parler immédiatement aux personnes autour d'elles, de valider auprès de leur hiérarchie avant de valider l'opération. La société a également été victime de faux emails interne avec une adresse PMU et la photo du Président. Cet email était une parfaite imitation cependant, ce n'était pas une pratique normale. C'est **cette traque constante de toute situation sortant de la norme** qui permet aux équipes de déjouer ces tentatives depuis de nombreuses années.

Par exemple, de faux emails de banques au moment des tests SEPA ont été reçus afin de procéder à des envois de fichiers tests. Mais aussi des fournisseurs qui mandataient des sociétés d'affacturage pour des changements de RIB. Là encore la consigne est simple, le PMU ne procède à aucun changement sans avoir pris contact avec l'interlocuteur habituel afin de vérifier l'exactitude de la demande.

Parfois certaines banques font une demande de changement des lignes ebics sans signer leur demande ou alors par un interlocuteur inconnu avec uniquement le logo de la banque. Il est important d'être méfiant et de toujours vérifier l'exactitude d'une demande avant de valider une opération.

Les fraudes peuvent également intervenir du coté bancaire. Les banques signalent régulièrement de faux appels du président du PMU. Cette tentative a été l'occasion de rappeler aux équipes bancaires leurs interlocuteurs habituels au sein du PMU. Contrer ce type de fraude passe aussi par une limitation du nombre de personnes habilitées et une attribution de pouvoirs spécifiques en fonction des comptes.

Si cela représente une contrainte d'un point de vue opérationnel, cela permet la mise en place de points de vigilance complémentaires tant au niveau des banques qu'en interne.
Concernant la fraude interne, des règles de signatures simple / double, en fonction du seuil, du compte ont été mises en place.

C'est également ne pas laisser la même personne gérer la trésorerie ou simplement renouveler et changer les équipes. Le travail en binôme / trinôme est aussi une sécurité. La multiplication des contrôles humains et l'automatisation des process afin de limiter le manuel font partie des procédures de luttes contre la fraude.

On constate une professionnalisation de la fraude non pas par les techniques mais par la connaissance des processus financiers. En effet, récemment de fausses circularisations de lettres de commissaire aux comptes circulent, ce qui prouve que les fraudeurs connaissent également les process complexe d'audit.

La lutte contre la fraude est quotidienne et in nie. Même si les fraudeurs sont de plus en plus inventifs, la communication, l'humain et l'ensemble des bonnes pratiques évoquées peuvent les contrer efficacement.

Valérie DURAND-FANTUZZI
Responsable Dpt Trésorerie, Moyens de Paiements & Assurances PMU

02 RETOUR D'EXPÉRIENCE : **TÉMOIGNAGE DU STORMSHIELD**

Stormshield fait de la communication un outil majeur

Juillet 2013 Stormshield enregistrait sa première tentative de fraude.

Il y a trois ans la fraude au président et plus largement la fraude en général n'était pas un sujet particulièrement traité dans les médias comme aujourd'hui. Les entreprises même spécialisées dans la sécurité comme Stormshield n'étaient pas vraiment à l'écoute de ces choses-là.

En juillet 2013 suite à la cession de la société, un nouveau président a été nommé. Aujourd'hui, on constate que des cas de fraude interviennent souvent à la suite d'un changement d'organigramme, de modification juridique de l'entreprise ou en période de congés. Stormshield réunissait plusieurs de ces critères dont la période et le changement de président.

Une personne de l'équipe comptable qui avait la capacité, à l'époque, de pouvoir opérer des virements en toute autonomie reçoit un email de l'adresse du président de la société.

Ci-dessous la retranscription du mail reçu :

Bonjour Anne,
J'espère que vous allez bien. Je m'adresse à vous dans le cadre d'une ***opération financière très confidentielle*** *que nous sommes en train de mener, et pour laquelle nous devons* ***transférer impérativement*** *aujourd'hui la somme de 300 000 euros en dépôt de garantie. Il s'agit d'une opération d'acquisition d'une société cotée en Asie, cette opération est donc extrêmement* ***confidentielle*** *et je m'adresse exclusivement à vous pour vous demander de réaliser ce virement aujourd'hui,* ***vous ne devez en parler à personne*** *au sein de la société pour ne pas* ***risquer de faire échouer l'opération,*** *ni même à Pierre-Yves.*

Vous allez recevoir ce matin un mail de notre ***cabinet d'avocats*** *qui va vous communiquer les références bancaires pour effectuer le virement.*

Une fois encore, ***j'insiste sur le caractère confidentiel de cette opération,*** *vous êtes la seule personne informée et je compte sur vous pour réaliser ce virement aujourd'hui.*

Bonne journée,
François ...

Les fraudeurs mettent l'accent sur l'aspect **urgent et confidentiel de l'opération.** Suite à ce premier échange, un mail d'un cabinet d'avocats prestigieux est envoyé afin d'appuyer le caractère professionnel et confidentiel de la demande.

Ci-dessous la retranscription du mail reçu.

Mademoiselle,
Vous avez dû recevoir un message de Monsieur François ..... qui vous a informé de l'opération d'acquisition pour laquelle nous vous conseillons. Comme convenu, vous trouverez ci-dessous les coordonnées bancaires du compte sur lequel vous devez effectuer le virement de 300 000 euros impérativement aujourd'hui.
Monsieur François ..... vous a fait part du caractère extrêmement confidentiel de cette opération, vous ne devez donc en parler à personne, et nous comptons sur vous pour réaliser ce virement aujourd'hui.
Dès que vous l'aurez effectué, je vous remercie de bien vouloir nous le confirmer par retour de mail.
Bien cordialement, Cabinet d'Avocats .....

Nous constatons que les fraudeurs appuient de nouveau avec cet email sur l'aspect confidentiel de l'opération. C'est l'insistance des fraudeurs sur le caractère confidentiel de l'opération qui a poussé la victime de cette fraude à faire part de ces doutes à sa hiérarchie.

Il y a 3 ans, peu de société victimes de tentatives de fraude portaient plainte. Cela a cependant permis à Stormshield de mettre en place un certain nombre d'actions. La société a **communiqué massivement** en interne et pas uniquement auprès du service financier. Des opérations similaires peuvent en effet avoir lieu sous d'autres formes dans d'autres services. Nos équipes sont sans cesse sensibilisées au risque de fraude par le biais d'articles de presse qui sont mis à leur disposition ou encore de formations.

Des process ont également été mis en place avec un système de double authentification, par exemple. Même si ce système peut paraître contraignant, il est néanmoins nécessaire. Stormshield a depuis 2013 essuyé deux autres tentatives. Ce que nous constatons dans ces différentes tentatives c'est que tout repose sur l'humain et la vigilance de chaque employé. Les process sont primordiaux mais ce n'est pas suffisant ! Cette tentative en 2013 a été déjouée uniquement parce que la personne a osé parler.

Dans les grands groupes nous constatons souvent que la victime n'ose pas venir interroger son N+1 ou N+2 lors de la réception d'email ou d'appel suspect. Il est primordial de développer le « Speak up » c'est-à-dire que peu importe le niveau de hiérarchie de la personne, elle ne doit pas avoir peur d'interpeller son management lorsqu'elle se retrouve face à une interrogation.

La lutte contre la fraude c'est briser l'isolement des victimes a n de déjouer les fraudes quasi quotidiennes que chaque entreprise peut subir.

Pierre-Yves HENTZEN
Directeur Administratif & Financier/CFO de la société Stormshield et président DFCG Rhône-Alpes Auvergne

03 ÉTHIQUE / **HUMAIN**

Charte Éthique quelle influence ?

Que cela soit dans un contexte de fraude interne ou externe, la responsabilité du salarié victime ou fraudeur est toujours engagée. Les conséquences en terme sociales et humaines peuvent être extrêmement lourdes. On parle ici de licenciement, cessation d'activité d'une entreprise, employés victimes en dépression... La notion de responsabilité est primordiale. Au sens légal du terme, la victime de fraude ne verra pas sa responsabilité mise en cause, on va alors se tourner vers l'entreprise qui a potentiellement les moyens financiers d'absorber la fraude contrairement à l'employé « lambda ». Cependant, aux yeux de l'entreprise, la victime d'une fraude au président est considérée comme responsable. Il ne viendrait jamais à l'idée de considérer comme responsable une victime de braquage. Une victime de fraude rencontre de nombreuses difficultés pour se faire reconnaitre socialement un réel statut de victime.

Une attaque fulgurante !

Le principal mode de fonctionnement des fraudeurs consiste à enfermer leurs victimes dans un tunnel psychologique a n de les isoler. « Confidentiel », « Urgent », la victime est isolée et se retrouve dans l'obligation. La durée d'une attaque n'excède pas 3 minutes. C'est 1 minute pour faire tomber les barrières psychologiques et 2 minutes pour mettre en confiance.

Le code éthique, une solution ?

Si l'on interroge les salariés européens, 89% souhaitent la mise en place d'un code éthique et 70% y voient un moyen efficace de prévenir la fraude. 25% des fraudes détectées le sont via un dispositif d'alerte. On note cependant, un décalage entre la France et les autres pays européens. 55% seulement des salariés français voient dans le code éthique un moyen de prévenir la fraude.

Au-delà de l'exception française voyons les causes réelles de cet écart :

La première raison est à trouver dans l'origine des chartes éthiques. Généralement, celles-ci ont été mises en place sous pression commerciale. Afin de finaliser un contrat, le partenaire commercial peut imposer la signature d'une charte éthique, la leur ou celle de l'entreprise. Il est à noter que les entreprises françaises préfèrent majoritairement produire leur propre charte. On constate donc une grande disparité dans les chartes éthiques certaines font 5 pages quand d'autres en comptent 50.

La deuxième raison vient d'un déficit de communication. Pour exemple, 1 salarié sur 3 n'a jamais signé la charte éthique quand il en existe une. Il n'y a donc rien qui assure que le salarié ait eu connaissance de son contenu.
La dernière raison provient du manque d'information quant au droit et devoir d'alerte. Le salarié ne sait pas comment exercer ce droit ni quels sont les relais dont il dispose pour donner l'alerte en cas de situation anormale.

Il est indéniable que la charte éthique est un moyen efficace de lutte contre la fraude et l'isolement des salariés face à celle-ci, si et seulement si ...

> Le contenu de la charte rappel les valeurs de l'entreprise, les règles générales et surtout mentionne les comportements attendus, ceux sanctionnés et le traitement de ces dérives. La charte doit également comporter une information détaillée sur les relais mis à disposition de tous les salariés afin de les rassurer et de les accompagner dans une situation inconfortable. Ces relais sont bien entendu faits par le Management dans un premier temps mais également la mise en place d'une hotline éthique (autorisée par la CNIL). Cette hotline éthique a l'avantage de préserver l'anonymat.

> Un contenu adapté ne suffit cependant pas, il est primordiale de le relayer auprès de tous les salariés et bien entendu à tout nouvel embauché. Au-delà d'une simple signature en bas de page, la formation continue des employés aux mécanismes de la fraude et sur les relais mis en place par l'entreprise sont plus que nécessaires.

La communication est le maître-mot d'une lutte contre la fraude efficace. Communiquez en amont, communiquez en cas de tentative de fraude, communiquez sur les cas passés et les nouvelles techniques de fraude recensées, communiquez !
Un contenu adapté, une communication efficace et une formation continue ne seront qu'un coup d'épée dans l'eau si à côté de cela il n'y a pas l'exemplarité.
C'est au management et à la direction d'une entreprise de montrer l'exemplarité à tout moment.

« Un homme averti en vaut deux ! »

Renforcer l'éthique par la mise en place d'une charte permet de lutter sur tous les fronts contre la fraude. Cela permet de faire de la prévention, de la dissuasion dans des cas de fraude interne et de la détection. Pour finir, un engagement éthique réussit c'est proposer à ses salariés des relais et de les protéger contre l'isolement favorisant la fraude.

Il ne faut pas oublier que 86% des fraudes sont déjouées grâces aux réactions humaines.

Isabelle CATUSSE
Vice-présidente de la Commission Fraude AFTE et Responsable Trésorerie Groupe Guerbet

04 QUAND LA CYBER SÉCURITÉ CONTRIBUE À **L'ENCHANTEMENT CLIENT**

Ou l'art de transformer une contrainte en bénéfice client

Au-delà de la technologie, la cyber sécurité nous protège avant tout de problèmes humains.

A cet égard, le fraudeur peut endosser tous les profils : pirate ou faussaire, collaborateur indélicat, client peu scrupuleux... Il est évident que des mesures fortes de protections face aux nombreuses menaces doivent être prises, dans un contexte relationnel omni-canal complexe. Il n'en reste pas moins que **le succès de ces mesures contraignantes relève avant tout de l'humain.**

Pour réussir, il convient d'abord de prendre en compte 3 paramètres essentiels : la concurrence que vous inspirez, les valeurs que vous portez et la conformité de vos méthodes aux habitudes de sécurité établies.

> **L'enchantement client repose d'abord sur la confiance.** Mais instaurer la confiance est une posture parfois contradictoire avec la surveillance tatillonne des comportements et des systèmes... Il importe donc de trouver le juste équilibre entre une attitude bienveillante et un regard soupçonneux ! Comme la confiance n'exclue pas le contrôle, l'équilibre se crée entre l'attitude responsable de l'entreprise et de ses collaborateurs, perceptible avec la symétrie des attentions[1] , et les moyens protecteurs visibles ou invisibles dans le parcours clients qui dissuadent les fraudeurs. Ainsi la cyber sécurité devient un élément de réassurance qui ne bloque pas les échanges. Le 3D Secure donne un exemple de l'équilibre à créer entre le besoin de sécuriser simplement les paiements online et la protection efficace du client et du marchand.

> **Le client est sensible aux valeurs de l'entreprise,** portées par l'ensemble des collaborateurs, et exprimées publiquement par la plateforme de marque. L'attitude responsable des collaborateurs permet souvent, avec bon sens, de repérer les situations suspectes. L'entreprise doit aussi s'engager à protéger les données de ses clients aussi sérieusement qu'un secret affectif. Et, malgré toutes ses précautions, l'entreprise est victime de fraude, la transparence et l'endossement des responsabilités sont les seules attitudes possibles : les décideurs doivent avoir conscience de ces enjeux pour prendre les mesures préventives et curatives.

> **Le client ne doit pas être dérouté par des mesures sécuritaires qu'il ne comprend pas.** Collectivement, les acteurs de l'écosystème appliquent des standards communs de protection et, par un usage récurrent, ils deviennent familiers et rassurants. Par exemple, le paiement sans contact n'exige plus de saisie de code pour régler des petits montants en magasin mais la sécurité reste assurée par les acteurs et schémas bancaires. Le client paye vite et simplement, mais en cas de fraude, c'est la banque émettrice qui sera responsable et non le porteur de la carte.

FACE AUX CONTRAINTES DE SÉCURISATION DES DONNÉES ET DES TRANSACTIONS, **IL EST ENCORE POSSIBLE DE CRÉER L'ENCHANTEMENT POUR VOS CLIENTS...**

L'enchantement, c'est le contraire de la « prise de tête » ! Autant votre client peut comprendre que vous preniez des précautions pour le protéger, et évidemment protéger votre organisation, autant il n'acceptera pas facile- ment de se compliquer la vie pour pouvoir traiter avec vous... surtout si vos concurrents sont plus habiles à le satisfaire en toute sérénité.

Confiance établie, valeurs de marques affirmées et cinématiques familières sont des éléments forts de réassurance. Pour passer à l'enchantement, il faut s'intéresser à l'expérience client telle qu'elle est vécue à travers vos canaux relationnels et à l'attitude que votre organisation adoptera à chaque étape de ces parcours.

Pour atteindre cet objectif avec vos équipes, il est nécessaire de décortiquer chaque étape de vos parcours client pour **détecter les irritants et rechercher les alternatives positives :**

- depuis le moment où vous établissez une relation, par exemple lors de la collecte d'informations personnelles de la KYC[2] ;

- au cours de la relation commerciale, et en particulier pendant les moments sensibles : accès à un espace sécurisé, recueil du consentement (signature), transaction sous toutes ses formes et mise à dis- position de services dématérialisés ;

- et, pour toute anomalie, en identifiant clairement les responsabilités et préjudices, et en mettant en œuvre sans délais les moyens pour y remédier. L'enchantement se produit si, sur tous les canaux, le parcours proposé à vos clients reste clair, homogène et de qualité constante, y compris dans les phases sensibles. La segmentation est aussi importante pour s'adapter au profil du client et l'ancienneté de la relation.

L'aboutissement de ces travaux doit permettre de **concilier des attitudes antinomiques** en favorisant la simplification et l'ouverture d'esprit, tout en améliorant constamment les techniques automatiques de scoring pour repérer immédiatement ce qui est suspect. Il faut également, du point de vue managérial, inciter les collaborateurs à une vigilance responsable, et créer la réciprocité des contrôles internes pour ne pas isoler les individus ou les systèmes d'alertes. Le client doit ressentir le sérieux de votre organisation sans être importuné par vos règles de sécurité, et la relation ne doit pas pâtir de postures anxiogènes.

En résumé, pour produire l'enchantement autour de la cyber-sécurité, plusieurs actions doivent être menées, globalement et simultanément, puis améliorées constamment, afin de :

> Développer l'attitude appropriée de vos collaborateurs, dans les phases sensibles : bienveillante mais attentive, souriante mais maligne, décontractée mais rigoureuse, etc. et, du point de vue managérial, évaluer la nature de chaque risque et les enjeux (réciprocité des contrôles).

> Mettre en place les outils appropriés à la dématérialisation et la sécurisation des données et des échanges : cryptographie, tokenization, coffre-fort numérique, tiers de confiance (ex. : ANTS), etc.

> Adopter de bonnes pratiques relationnelles : confirmation systématique des transactions, alertes SMS si nécessaire (mais sans abuser), cinématiques de sécurité éprouvées, etc.

Il vous appartient désormais de transformer vos contraintes cyber-sécuritaires en bénéfices clients.
Nous pouvons vous aider concrètement, et vous avez tout à y gagner !

François LECOMTE-VAGNIEZ
Associé Lobary (www.lobary.com)

[1] Le concept de «symétrie des attentions» postule que la qualité de la relation entre une entreprise et ses clients est égale à la qualité de la relation de cette entreprise avec ses propres collaborateurs. Source : JDNet.

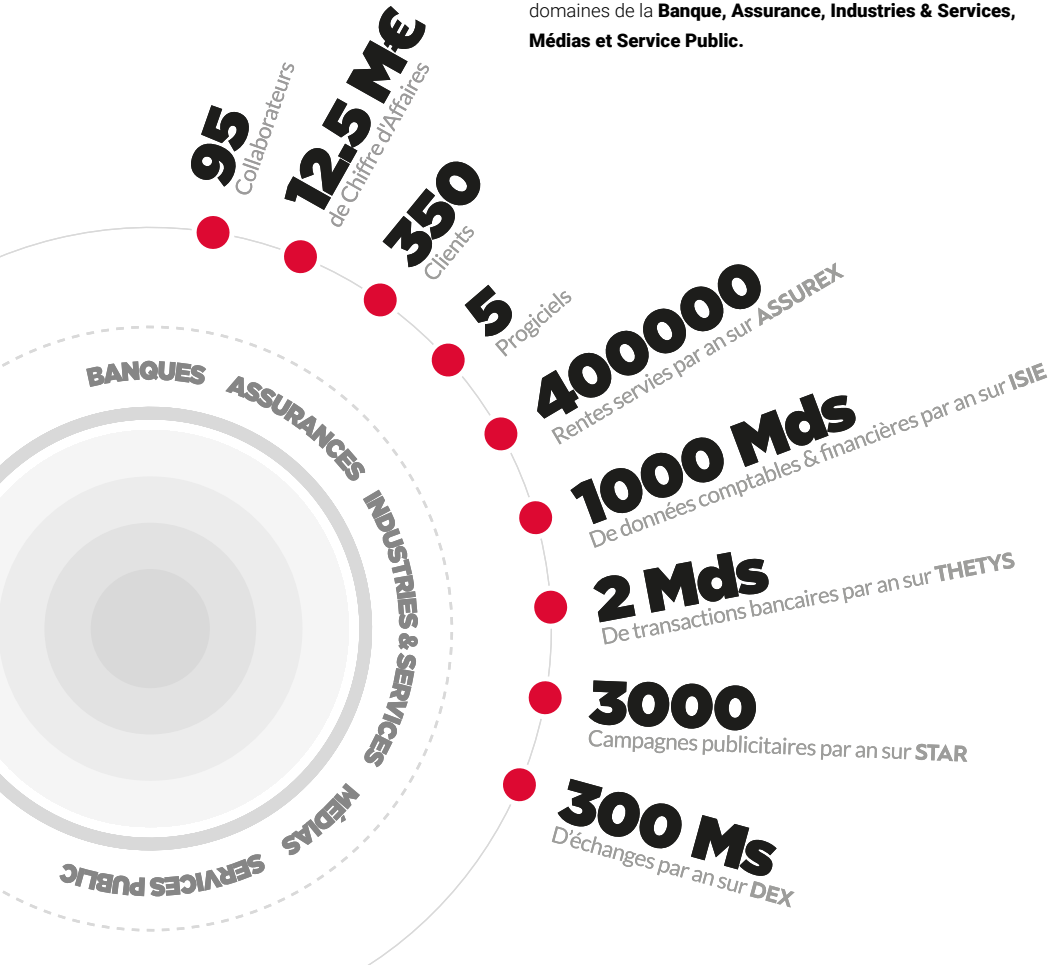
[2] Know Your Customer (KYC) est le processus consistant, pour une entreprise (en particulier les banques, assurances, télécoms, etc.), à vérifier l'identité de tout prospect avant l'ouverture d'un service.

La **lutte contre la fraude** est un **sujet d'actualité** pour vous ?

Expert en **gestion de flux** & spécialiste des **processus de gestion**

NOS EXPERTISES & SAVOIR-FAIRE

Nos solutions progicielles sont proposées en mode **SaaS**, pour garantir à nos clients une réponse automatique aux évolutions métiers, règlementaires et techniques dans les domaines de la **Banque, Assurance, Industries & Services, Médias et Service Public.**



ISIE

Gestion des flux comptables et financiers et gouvernance des données financières.

THÉTYS

Gestion de la trésorerie : gestion des moyens de paiement, des pouvoirs bancaires et cash management.

ASSUREX

Gestion des Rentes et des contrats d'Assurance Epargne / Prévoyance.

DEX

EAI : Gestion des flux inter applicatifs, les données sont transportées, transformées, et supervisées automatiquement

STAR

Gestion, pilotage et optimisation du cycle de vie des ventes d'espace « print », « digital » et « hors media ».

W W W . A C A . F R

https://www.linkedin.com/groups/3967314/profile

https://twitter.com/aca_tweet

http://www.aca.fr/blog-aca

CONTACTEZ NOUS

marketing@aca.fr
01 53 53 80 80
69 rue Monceau, Paris 75 008 France