الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ ع إ م

LETTRE D'INFORMATION : BON A SAVOIR (N°34)

Faut-il avoir peur d'internet ?

Non bien sûr ! Les risques sont à appréhender comme ceux de la vie courante. Mais mieux les connaître, c'est mieux s'en protéger ! Apprenez à les identifier

Le phishing

Le phishing (ou hameçonnage et parfois filoutage), est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc.

C'est une forme d'attaque informatique reposant sur l'ingénierie sociale (sécurité de l'information). Le phishing peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.

Les mules

Une « mule » est le nom donné à une personne utilisée pour transporter des matériaux illicites : explosifs, armes, drogues, parfois à son insu.

Sur Internet, les mules sont "recrutées" par e-mail pour "transporter de l'argent" contre rémunération. Pour la recruter, le pirate abuse un internaute qui se rend ainsi complice d'une fraude (vol, détournement ou blanchiment d'argent) passible de poursuites.

Le pharming

Le pharming (ou dévoiement en français) est une technique de piratage informatique exploitant des vulnérabilités DNS. Cette technique consiste à détourner l'accès à un site Internet vers un site pirate. L'URL est correcte, mais l'internaute est sur un faux site. Les informations confidentielles saisies sont capturées par le pirate.

Le spam

Le spam, pourriel ou polluriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

Le phishing et les canulars utilisent en partie cette technique.

Les arnaques et canulars

A l'instar du spam, une arnaque est un e-mail que vous n'avez jamais demandé à recevoir et qui vous propose en général un gain d'argent facile et rapide (loterie, bourse, etc.) ou qui sollicite votre compassion.

Dans certains cas, l'arnaque peut consister à faire de vous une mule. Mais attention, vous devenez complice du pirate, de ses malversations et vous risquez gros.

Les canulars (appelés hoax en anglais) se trouvent souvent sous la forme de courriel ou de simple lettre-chaîne. Dans ce dernier cas, Internet ne fait qu'amplifier un phénomène qui existait déjà à travers le courrier traditionnel. À la différence des

spams qui sont la plupart du temps envoyés de manière automatisée à une liste de destinataires, les canulars sont, eux, relayés manuellement par des personnes de bonne foi à qui on demande de renvoyer le message à toutes ses connaissances, ou à une adresse de courrier électronique bien précise.

Les virus

Un virus informatique est un logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc.

Les spywares

Un spyware est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

Les chevaux de Troie

Un cheval de Troie est un logiciel d'apparence légitime conçu pour exécuter subrepticement (de façon cachée) des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

Windows Live Messenger, le téléchargement de programmes gratuits et le partage des programmes ou autres fichiers sont les principales sources de diffusion des chevaux de Troie. Ils sont également très fréquents dans certains types de courriels.

Les informations transmises

Lorsqu'on utilise les services d'un site Internet, des informations souvent personnelles sont transmises (e-mail, nom, prénom, identifiant, mot de passe, N° de carte bancaire, etc.).

Pour être certain de communiquer en toute sécurité avec son site bancaire ou d'achat en ligne, quelques précautions et vérifications s'imposent.

https://bpnet.gbp.ma/securite/securite1.asp

La sécurisation du système d'information

Les particuliers et les professionnels qui détiennent des fichiers informatiques ont l'obligation d'assurer la sécurité de leurs données selon la loi informatique et liberté.

La protection de ces informations peut prendre plusieurs formes.

Mise en place d'une stratégie de mot de passe sérieuse

La mise en place d'un système d'identifiant et de mot de passe constitue la première protection à instaurer sur un poste de travail. Ces deux paramètres devront être confidentiels, individuels et difficiles à déchiffrer. Chaque utilisateur devra se faire aider par un spécialiste, le responsable informatique par exemple dans le cadre de l'entreprise, pour le choix du mot de passe.

En général, le mot de passe devra comporter au moins huit caractères formés par des chiffres, des caractères spéciaux et des lettres. Il devra être changé régulièrement, à chaque trimestre par exemple. Chaque mot de passe devra être différent des précédents afin de garantir un maximum de sécurité.

Assurer une meilleure gestion des comptes utilisateurs

Il n'est pas rare qu'un employé quitte l'entreprise pour diverses raisons.

L'instauration d'une bonne gestion des comptes utilisateurs permettra de mieux sécuriser les données de la société. Cette procédure passe par l'usage d'une adresse électronique nominative et non générique. C'est également un bon moyen de responsabiliser chaque utilisateur et de mieux tracer l'historique de la manipulation des fichiers sensibles. Tout le monde devra être mis sur le même pied d'égalité même les administrateurs du système et des réseaux informatiques de l'entreprise.

Sécurisation du poste de travail

Il arrive que l'utilisateur doive s'absenter de temps à autre de son poste de travail. Afin de ne pas exposer les fichiers au regard indiscret, il est important de paramétrer le verrouillage automatique du système après quelques minutes d'inactivité. Chacun devra également acquérir le réflexe de verrouiller son poste de travail lorsqu'il sera amené à se déplacer même pour un laps de temps court. L'objectif est d'éviter les éventuels fraudes et les abus dont il pourrait être victime.

Il est également conseillé de contrôler l'utilisation des ports USB d'un poste de travail contenant des données sensibles. Le but est par exemple d'interdire toute copie de fichiers vers ces périphériques. Sinon, il est également possible de restreindre les personnes pouvant accéder aux documents confidentiels et de les modifier ou d'en faire une copie.

Protection des données contre les attaques extérieures

Les menaces informatiques pesant sur le poste de travail et les données qu'il contient sont nombreuses : spam, virus, cheval de troie, phishing, déni de service, etc. Pour les contrer, il faudra penser à mettre en place des filtres anti-spam et anti-virus efficaces en amont sur le serveur ou carrément sur le poste de travail. Leur mise à jour devra se faire automatiquement.

La messagerie électronique devra faire l'objet d'une surveillance particulière et étroite. C'est par cette voie que la plupart des menaces pénètrent dans le système informatique de l'utilisateur. Les spams reçus chaque jour pourraient être bénins ou contenir des logiciels malveillants. Ces derniers porteraient préjudice à toutes les données informatiques de l'utilisateur s'il n'est pas vigilant.

https://fqdn.fr/2014/06/03/la-securisation-du-systeme-dinformation/

Utiliser l'analyse des données pour lutter contre la fraude et la criminalité financière

Les hackers et les fraudeurs développant des techniques de plus en plus sophistiquées, les assureurs doivent eux aussi se servir de l'apport de dernières avancées technologiques pour tenter de juguler ces activités criminelles. Les clients veulent que leurs coordonnées bancaires et personnelles soient suffisamment protégées, et qu'en cas de fraude les fraudeurs soient identifiés.

Les assureurs doivent se protéger des menaces concernant l'appropriation des données confidentielles, telles que les données personnelles des assurés, et doivent lutter contre les déclarations d'indemnisation frauduleuses.

Un océan de données

Les assureurs obtiennent des données de multiples provenances, à la fois structurées (de la part des assurés), et non structurées (de la part des médias sociaux, de tiers, etc.).

Gérer ces données, s'assurer de leur pertinence, à une juste fréquence, et les rendre accessibles à ceux qui en ont besoin, est un défi majeur.

Il est indispensable pour les assureurs de bénéficier d'une vision intégrée des données : ce qui suppose des systèmes centralisant les informations qui fournissent une vue unique du client et de ses relations avec l'assureur, en lien avec les autres sources de données clés, tel que les bases de données externes.
Dans la plupart des cas, l'information a été obtenue et stockée indépendamment, dans différents départements.
Dans d'autres cas, des informations précieuses sécurisées, provenant des médias sociaux par exemple, peuvent être utilisées dans des buts commerciaux, mais non partagées avec les équipes en charge de la lutte contre la fraude.
Les recherches d'Accenture montrent qu'un peu plus de la moitié des organisations financières ont une vue unique de leurs clients, et seulement la moitié environ ont un système unique pour se mettre en conformité avec les directives de lutte contre le blanchiment d'argent.
De même, les données liées à la gestion contre la fraude sont fragmentées entre les différentes filières et produits d'assurance.
En conséquence, mettre en place une gouvernance des données devient un objectif majeur pour les assureurs qui doit leur permettre de :
- mieux contrôler les flux de données et assurer leur protection, ce qui est un élément central de la gestion du risque de réputation.
- s'assurer de la fiabilité, de la qualité et de la cohérence des données, dont le volume entrant est chaque jour plus important, pour que leur utilisation puisse être un levier de croissance.

Combiner les données et l'analytics pour lutter contre la fraude et la criminalité financière

Les nouvelles technologies apportent des solutions pour faciliter le travail d'acquisition et d'intégration des données, dont de précieuses informations et analyses peuvent être tirées grâce à l'utilisation des techniques d'analyse les plus avancées.
Pour cela, les assureurs doivent disposer de trois choses :

Disposer de données de meilleure qualité.

La première étape d'amélioration de la qualité de données consiste à définir les métriques appropriées pour juger de leur qualité. Cela nécessite un ensemble cohérent de critères pour mesurer et améliorer la qualité des données, incluant l'exactitude et l'intégrité des données, leur complétude ou la capacité à les dater afin de vérifier si elles sont toujours à jour ou nécessitent une actualisation pour pouvoir être utilisées.
La seconde étape est de mettre en place un dispositif de réconciliation et d'analyse des données. Un filtrage et un nettoyage approprié des données améliorent la qualité de l'analyse et aident à réduire le nombre de faux-positifs.
La troisième étape est d'améliorer le dispositif de gouvernance des données.
Beaucoup d'assureurs disposent désormais d'un «□ Chief Data Officer□ ». Une gouvernance des données, avec des règles bien définies concernant la propriété des données et leur qualité, est un point de passage nécessaire pour coordonner les différents acteurs.

Utiliser «l'analytics» pour transformer les données en information, et l'information en analyse.

Plus encore que le manque de données, le vrai défi est le manque de «□ bonnes□ » données, c'est-à-dire trouver les données utiles parmi un flux croissant de nouvelles données arrivant constamment.
La plupart des institutions financières utilisent moins de 5□ % de leurs données disponibles pour prendre des décisions relatives à la prévention contre la criminalité financière.

Les techniques d'analyse vont permettre d'utiliser ces données brutes pour en tirer des enseignements. La mise en place d'un modèle de scoring, l'analyse prédictive, ou l'analyse de données textuelles («□ text mining□ »), par exemple, peuvent accroître le champ d'informations pouvant être tirées des données.
Cela peut aider l'assureur à comprendre un risque posé par un problème spécifique à un client ou à un type de produit, ou à identifier avec plus de précision les cas de sinistres à investiguer.

Utiliser des techniques de visualisation des données.

En réponse au volume et à la complexité croissante des données, des techniques de visualisation permettent à des données complexes d'être visualisées et interprétées par les experts du métier via une interface visuelle. Cela les aide à identifier des scénarios et des incohérences.
Par exemple, une fois qu'un contrat d'assurance est ouvert, il y a une surveillance continue pour repérer d'éventuelles opérations suspectes. Un éclairage visuel sur les flux d'opérations liées aux contrats aide les investigateurs à identifier de nouveaux scénarios de fraude, par exemple quand différents sinistres ou prestations proviennent d'un même prestataire.

Les avantages d'une meilleure gestion des données

Étant donné le volume important et croissant d'opérations à contrôler, les investigateurs les plus chevronnés ont des difficultés à absorber l'accroissement du nombre de données et d'opérations à traiter selon les approches traditionnelles.
Atteindre l'idéal d'une vue unique et exhaustive de chaque client pour aider à détecter et empêcher la fraude et la criminalité financière, peut aider les assureurs à réduire le risque de non-conformité.
Ils peuvent ainsi prendre de meilleures décisions de manière préventive lors de l'évaluation des risques, ou l'identification des cas de sinistres à investiguer.
Les technologies émergentes peuvent être utilisées pour tirer de l'information des analyses de mails, des messages vocaux et même des messageries instantanées.
De plus en plus de clients communiquant directement avec leur assureur via des canaux digitaux et mobiles, la capacité à reconnaître précisément un appareil spécifique et ses accès, peut être extrêmement importante pour pouvoir empêcher les cyberattaques.
Une vue unique sur le client permet aussi de rendre plus facile la vente croisée, améliorer la qualité de service, et augmenter le taux de fidélisation du client, grâce à une meilleure compréhension des acteurs avec qui les assureurs interagissent.

Assureurs et lutte contre la criminalité financière

Dans un article publié sur le site "Décideurs" et intitulé "Utiliser l'analyse des données pour lutter contre la fraude et la criminalité financière", Philippe Lefèvre, senior manager Finance & Risk, et Heather Adams, managing director Finance & Risk chez Accenture expliquent comment les assureurs doivent se prémunir contre les attaques de hackers et de fraudeurs et protéger les données de leurs clients.
Les clients des assureurs craignent pour leurs données personnelles qui sont parfois hackées par des fraudeurs et donnent lieu à des déclarations d'indemnisation frauduleuses.
Pour les auteurs, il est indispensable d'avoir une vision intégrée des données collectées car celles-ci proviennent de multiples plateformes, structurées ou non, "ce qui suppose des systèmes centralisant les informations qui fournissent une vue unique

du client et de ses relations avec l'assureur, en lien avec les autres sources de données clés, tel que les bases de données externes."
Or, d'après les recherches menées par Accenture, "un peu plus de la moitié des organisations financières ont une vue unique de leurs clients, et seulement la moitié environ ont un système unique pour se mettre en conformité avec les directives de lutte contre le blanchiment d'argent."
Il est nécessaire pour ces entreprises de mettre en place une gouvernance des données, de manière à mieux contrôler les flux de données et assurer leur protection d'une part et s'assurer de la fiabilité, de la qualité et de la cohérence des données d'autre part.
Pour mener à bien la lutte contre la fraude et la criminalité financière, elles doivent combiner les données et l'analytics.
Pour cela, selon les auteurs, les assureurs doivent "définir les métriques appropriées pour juger de leur qualité. Cela nécessite un ensemble cohérent de critères pour mesurer et améliorer la qualité des données, incluant l'exactitude et l'intégrité des données, leur complétude ou la capacité à les dater afin de vérifier si elles sont toujours à jour ou nécessitent une actualisation pour pouvoir être utilisées.
La seconde étape est de mettre en place un dispositif de réconciliation et d'analyse des données. Un filtrage et un nettoyage approprié des données améliorent la qualité de l'analyse et aident à réduire le nombre de faux-positifs.
La troisième étape est d'améliorer le dispositif de gouvernance des données.
Beaucoup d'assureurs disposent désormais d'un «Chief Data Officer». Une gouvernance des données, avec des règles bien définies concernant la propriété des données et leur qualité, est un point de passage nécessaire pour coordonner les différents acteurs."
Il est important de noter qu'aujourd'hui, les institutions financières utilisent moins de 5% de leurs données disponibles pour agir sur leur politique de prévention contre la criminalité.
D'où la nécessité d'utiliser davantage des données brutes, de mettre en place un modèle de scoring, d'analyse prédictive et de text mining (analyse des données textuelles).
Enfin, pour répondre au volume croissant des données, ces entreprises doivent développer leurs propres outils de visualisation des données de manière à identifier clairement les différents scénarios et détecter des incohérences ou opérations suspectes.

Prévention du blanchiment : comment gérer l'approche par les risques ?

La mise en œuvre d'une approche par les risques pour la prévention du blanchiment est complexe : il faut établir une classification des risques *ad hoc*, l'appliquer aux clients, mettre en place des procédures de contrôle dans l'établissement, enfin rendre conformes les outils d'entrée en relation ou d'analyse comportementale. Les établissements seront-ils prêts à temps ?
La 3^{e} directive sur la lutte antiblanchiment et contre le financement du terrorisme, transposée en droit français par l'ordonnance de janvier 2009 et les décrets de juillet et septembre 2009, a constitué la principale préoccupation des correspondants Tracfin et responsables conformité des établissements bancaires et financiers dans les mois qui viennent de s'écouler.

Le questionnaire de lutte antiblanchiment à destination de l'Autorité de contrôle prudentiel (ACP) a également été revu et modifié pour intégrer les nouveautés réglementaires avec des questions qui parfois posent encore quelques problèmes d'interprétation aux établissements.

Ce questionnaire, rappelons-le, avait constitué au moment de sa mise en œuvre, il y a 10 ans, une excellente manière d'auto-évaluer les dispositifs des banques en la matière, mais cette cible apparaît désormais encore plus lointaine. Il sera, en effet, difficile pour la plupart des établissements de répondre positivement aux questions qui constituent le nouveau socle de la prévention du blanchiment.

Classification des risques : les grandes tendances

Le principal travail des établissements de crédit, comme des entreprises d'investissement, sociétés de gestion d'actifs et entreprises d'assurances, a consisté à mettre en œuvre une approche par les risques.

Les classifications de risques de blanchiment ont progressivement vu le jour, puisqu'il s'agit d'évaluer le risque, à partir des axes d'analyse prévus par la réglementation : nature des produits ou des services offerts, conditions des transactions proposées, canaux de distribution utilisés ainsi que caractéristiques des clients.

Si les caractéristiques des clients n'ont pas posé trop de problèmes pour les établissements, qui différenciaient pour certains, déjà, leurs niveaux de diligences en fonction du type de contreparties et de la domiciliation du client, en revanche, les autres axes ont posé plus de questions.

Concernant la nature des produits, certains d'entre eux considérés comme peu risqués par les textes réglementaires vont bénéficier d'une note de risque peu élevée puisque le régulateur estime qu'en l'absence de soupçons de blanchiment, les diligences prévues par les articles L. 561-5 et 6 du Code monétaire et financier (Comofi) ne sont pas à réaliser.

En revanche, l'appréciation est totalement laissée aux établissements quant aux autres produits, avec néanmoins un bémol : il apparaîtra difficile de justifier aux régulateurs un niveau de risque faible pour d'autres produits que ceux cités par les textes.

Par ailleurs, cette appréciation interne permettra d'alléger les mesures de vigilance en termes de suivi mais pas d'identification de la clientèle. Un niveau de risque plus élevé (par exemple, concernant des produits dérivés dans les activités de marché ou opérations en espèces) pourra être justifié par des typologies de cas de blanchiment intervenus sur certains produits et diffusés par le Gafi ou les CRF (Cellule nationale de renseignement financier, Tracfin en France).

Par ailleurs, il est indispensable de prendre en compte *a minima* les cas de risques forts cités par la réglementation.

Des mesures de vigilance complémentaires

En effet, des mesures de vigilance complémentaires sont notamment prévues dans les cas suivants :

- le client ou son représentant légal n'est pas physiquement présent ;
- les personnes sont politiquement exposées ;
- le produit ou l'opération favorise l'anonymat ;
- l'opération est pour compte propre ou pour compte de tiers effectuée avec des personnes physiques ou morales domiciliées dans un État ou un territoire dont les insuffisances de la législation ou les pratiques font obstacle à la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT).

Par ailleurs, on retrouvera dans l'axe d'analyse « canaux de distribution », le cas où le client n'est pas physiquement présent (risque fort) ou lorsque l'entrée en relation est réalisée par des apporteurs, qu'ils soient régulés ou non.

Enfin, l'axe qui a certainement posé le plus de questions aux établissements a été celui des « conditions des transactions ». En effet, dans le cas d'un client existant, cet axe pourra s'alimenter des anomalies éventuelles détectées par les systèmes d'alerte, mais pour un prospect, il n'y a guère que le comportement atypique du client qui peut constituer un indice.

L'expérience d'élaboration de nombreuses classifications de risques amène surtout à éviter de trop sophistiquer le dispositif et de garder en tête l'objectif de la classification qui est de différencier les diligences à l'entrée en relation en fonction des risques identifiés et bien sûr, de mieux cibler les alertes à analyser.

Actualiser les classifications de risque

Pérenniser et actualiser les classifications de risque est aussi un vrai sujet pour les établissements bancaires et financiers.

Pour un client qui est à l'initiative d'opérations ou de produits qui n'étaient pas prévues au départ, il faudrait effectivement réappliquer la classification pour obtenir une notation actualisée en fonction des produits réellement utilisés par le client.

Mais cette actualisation suppose une interface entre l'outil d'analyse comportementale par exemple et la classification des risques, certes nécessaire mais difficile à mettre en place rapidement.

Par ailleurs, la classification doit aussi évoluer sans délai dès qu'un nouveau produit est créé dans un établissement. Ceci suppose que les nouveaux produits soient notés en matière de risque LCB-FT lors des comités nouveaux produits, ce qui nécessite une modification des procédures nouveaux produits et du contenu des éléments analysés lors du comité, ainsi qu'un nouveau processus de transmission d'information entre ce comité et les personnes en charge de maintenir la classification des risques.

Dernier élément de complexité : l'homogénéité des classifications et des approches dans les groupes multi-activités dans lesquels, par exemple, une filiale productrice de contrat d'assurances entrant dans les critères de produits à risque faible n'aura pas la même classification des risques vis-à-vis de ce client qu'une agence du même groupe qui est susceptible de vendre des produits bancaires au même client.

Que manque-t-il aux établissements pour être prêts ?

• **Appliquer la classification au stock de clients existants**, compte tenu de l'état des données informatisées dans les établissements, est une tâche ardue et l'analyse des dossiers papier est difficilement faisable dans les délais impartis dans les grandes banques à réseau. C'est dire que beaucoup ne seront pas prêts et c'est pourquoi la priorisation est essentielle, mais aussi la simplicité de la classification.

Une des priorités consiste à repérer dans le stock de clients existants les personnes politiquement exposées (PPE), ce qui suppose de s'être équipé de l'une des bases de données de marché pour repérer plus facilement ces derniers.

• **Mettre en place des procédures adaptées** à la 3^{e} directive paraît plus simple et pourtant rien de plus compliqué que d'obtenir une procédure simple, compréhensible par tous les acteurs qui devront l'utiliser dans la mesure où les cas particuliers sont nombreux (diligences allégées envers certaines catégories de clients à appliquer sous réserve de vérifier qu'ils rentrent bien dans cette catégorie, diligences complémentaires quand le client ressort risqué et dans les cas cités par la réglementation, diligences faites par des tiers, en distinguant ces derniers car les diligences ne seront pas les mêmes si le tiers est un CIF ou un IOB par exemple…).

Dans le cadre de la mise en place de ces procédures, les établissements doivent désormais se référer non seulement au cadre législatif et réglementaire déjà cité, mais également aux modifications du CRBF 97.02 pour les établissements de crédit, de paiement et les entreprises d'investissement, la réglementation AMF pour les sociétés

de gestion d'actifs et les lignes directrices diffusées par les régulateurs et Tracfin et qui constituent les bonnes pratiques de la profession…

• **Mettre en conformité les outils** reste la tâche la plus ardue. De ce côté, les établissements auront du mal à être prêts à temps, car les sujets sont vastes :

- intégrer la classification des risques dans les outils d'entrée en relation n'est pas forcément une tâche aisée, surtout dans la banque de détail où les établissements hésitent à donner au chargé de compte l'accès à la classification des risques. Cette classification devra alors être utilisée dans les *back-offices* gérant les vérifications d'entrée en relation et celle-ci ne pourra être effective qu'une fois collectées les pièces qui correspondent à la cotation du client, cette entrée en relation en deux étapes ne simplifiant pas forcément les processus;

- mettre en cohérence l'approche par les risques et les outils d'analyse comportementale est également un véritable projet, dans un cadre où les établissements sont encore en cours de déploiement de leurs outils, soit à l'international ou dans certaines activités (comme les activités de marché).

On peut là encore procéder par étapes, la classification servant tout d'abord à prioriser les alertes à analyser avant d'intégrer totalement cette approche par les risques dans les fonctionnalités d'analyse comportementale servant à détecter automatiquement les cas atypiques. Par ailleurs, certains des indices de fraude fiscale définis dans le décret de juillet 2009 doivent aussi être rajoutés aux autres indices de blanchiment paramétrés dans ces outils.

Une amélioration durable des dispositifs

Face à ces enjeux et ces projets très lourds pour les établissements, il reste à espérer que l'application de ces dispositions améliorera durablement les dispositifs de prévention et permettra de lutter efficacement contre le fléau du blanchiment, but ultime de ces réglementations.