BANK INSIGHT

LA NEWSLETTER BANQUE DES CONSULTANTS SOLUCOM

AVRIL / MAI 2016 – N°6

EDITO

EH BROTHER

L'ouverture des systèmes d'information aux environnements externes et l'évolution des outils d'analyse des données permettent aujourd'hui d'accroître considérablement la connaissance clients et d'identifier leurs appétences et leurs besoins afin de leur proposer les produits les plus adaptés.

Une aubaine pour de nombreux secteurs marchands et une transformation radicale du champ du marketing.

La mise en place du Big data avec son aéropage de Data scientists est en marche, cette nouvelle « science » de la donnée ne doit bien sûr pas être faite « sans conscience ».

Gageons sur l'arsenal réglementaire et la déontologie bancaire pour éviter tout dérapage afin que le Big data ne devienne Big brother.

Olivier Schmitt

SOMMAIRE

TRAITEMENT DES DONNÉES ET SÉCURITÉ FINANCIÈRE : QUELLES PERSPECTIVES OPÉRATIONNELLES ? _ 2

COMPLIANCE AND BANKING "GENERAL DATA PROTECTION REGULATION" : LES ENJEUX DU SECRET _ 3

LE BIG DATA N'EST PLUS UNE PROMESSE MAIS UNE RÉALITÉ _ 4

LES CHIFFRES CLÉS / AGENDA _ 5

L'OFFRE SOLUCOM _ 6

BIG DATA ET SÉCURITÉ FINANCIÈRE : QUELLES CONVERGENCES ?

LES DONNÉES DÉTENUES PAR LES BANQUES FORMENT UN ENSEMBLE VASTE ET HÉTÉROGÈNE QUE L'ON NE RETROUVE DANS AUCUN AUTRE SECTEUR. ET POURTANT, L'ACCÈS AUX DONNÉES BANCAIRES ET FINANCIÈRES SE HEURTE À LA DISPERSION DES INFORMATIONS, À LEURS COÛTS D'ACCÈS, À LEUR PLUS OU MOINS BONNE QUALITÉ ET AUX DIVERSES CONTRAINTES RÉGLEMENTAIRES ET JURIDIQUES.

LE BIG DATA EST AINSI NÉ DE LA VOLONTÉ DES ÉTABLISSEMENTS D'EXPLOITER LES ÉLÉMENTS PERTINENTS CONTENUS AU SEIN DE CETTE QUANTITÉ ASTRONOMIQUE DE DONNÉES. LE TERME GÉNÉRIQUE DE BIG DATA DÉSIGNE DONC L'ENSEMBLE DES TECHNOLOGIES PERMETTANT DE STOCKER, D'EXPLOITER ET DE CORRÉLER LES MASSES D'INFORMATIONS ISSUES DU MONDE DE L'IT.

DANS LE SECTEUR BANCAIRE, C'EST DANS LE DOMAINE MARKETING ET COMMERCIAL QUE LES EXPÉRIENCES EN COURS SONT LES PLUS AVANCÉES, MAIS C'EST DANS CELUI DE LA SÉCURITÉ FINANCIÈRE QUE SONT OPÉRÉS LES GRANDS INVESTISSEMENTS. L'UN DES GRANDS ENJEUX POUR L'INDUSTRIE BANCAIRE EST DE MIEUX EXPLOITER SES PROPRES DONNÉES POUR CONTRER CE PHÉNOMÈNE. IL S'AGIT DE PASSER DU TRAITEMENT DES DONNÉES QUANTITATIVES À CELUI DES DONNÉES QUALITATIVES DONT IL FAUT RENDRE LE RÉSULTAT INTELLIGIBLE PUISQU'IL S'AGIT DE DONNER DU SENS À CETTE MASSE DE DONNÉES (CROISER DES INFORMATIONS ISSUES DE SOURCES DISTINCTES ET HÉTÉROGÈNES ET FOURNIR DES MÉCANISMES EFFICACES PERMETTANT DE RAPPROCHER AUTOMATIQUEMENT ENTRE EUX LES DIFFÉRENTS SIGNAUX D'ALERTES AFIN DE DÉTECTER EN TEMPS RÉEL LES « COMPORTEMENTS SUSPECTS »). MAIS POUR QUE LA MISE EN PLACE D'UN SYSTÈME DE BIG DATA SOIT EFFICACE, LES SERVICES DOIVENT COLLABORER ENSEMBLE. TRAITEMENT DES DONNÉES ET SÉCURITÉ FINANCIÈRE : QUELLES PERSPECTIVES OPÉRATIONNELLES ?

EN FRANCE ET EN EUROPE, L'UTILISATION DES DONNÉES PERSONNELLES EST TRÈS ENCADRÉE PAR LES TEXTES ET PRÉSENTE DES DIFFÉRENCES NOTABLES, NOTAMMENT AVEC LES ÉTATS-UNIS. COMPLIANCE AND BANKING "GENERAL DATA PROTECTION REGULATION": LES ENJEUX DU SECRET.

POUR RÉPONDRE À CE DÉFI, « LE BIG DATA N'EST PLUS UNE PROMESSE MAIS UNE RÉALITÉ » : LES BASES DE DONNÉES ET LES SOLUTIONS TECHNIQUES DÉDIÉES À L'EXPLOITATION MASSIVE DES DONNÉES SONT OPÉRATIONNELLES. ASSOCIÉES À L'APPROCHE HUMAINE, ELLES SONT CHOISIES ET DÉCLINÉES POUR ORGANISER LA CAPACITÉ PRÉDICTIVE DES BANQUES.

TRAITEMENT DES DONNÉES ET SÉCURITÉ FINANCIÈRE : QUELLES PERSPECTIVES OPÉRATIONNELLES ?

LES FONCTIONS CHARGÉES DE GARANTIR LA SÉCURITÉ FINANCIÈRE

(lutte contre le blanchiment et le financement du terrorisme, gel des avoirs et, selon les organisations, abus de marché et lutte contre la fraude) ont pris un véritable essor dans les établissements bancaires et financiers pour plusieurs raisons.

Aujourd'hui les groupes bancaires et financiers sont exposés à des montants de sanctions (de plusieurs centaines de millions à plusieurs milliards) tels que la dimension Groupe de la sécurité financière devient un enjeu opérationnel. Jusqu'à présent celle-ci ne représentait qu'un enjeu réglementaire.

Par ailleurs, après une dizaine d'années de superposition des sujets de conformité, auxquels ont répondu les établissements par des couches successives de solutions informatiques, une deuxième génération de dispositif est actuellement en cours de préparation, permettant de proposer une vision consolidée au niveau central.

Les enjeux judiciaires sont également devenus fondamentaux pour la pérennité d'un établissement. Risque de contentieux ou d'action en justice avec un client s'il soupçonne des manquements en matière déontologique, réglementation sur la protection de la clientèle en perpétuelle évolution, fraude sur les moyens de paiement, abus de faiblesse, fraude fiscale…

Tous ces enjeux rendent nécessaires deux types de besoins :

- la nécessité de piloter le risque et les activités de sécurité financière ;
- la nécessité de piloter la surveillance de l'activité au niveau central.

Si ces thématiques sont clairement identifiées par les établissements bancaires et financiers, nous pouvons constater qu'elles peuvent recouvrir plusieurs types de mise en œuvre opérationnelle.

PILOTER LE RISQUE ET LES MOYENS ALLOUÉS

Piloter la sécurité financière au niveau Groupe, c'est déjà évaluer et piloter les différents risques de manière consolidée.

Au-delà de la cartographie des risques, il s'agit pour les établissements de mettre en accord les dispositifs de surveillance avec les risques. Cette mise en adéquation requiert une évaluation des moyens alloués (système d'information, ressources humaines), la couverture des périmètres à surveiller, l'adéquation des scénarios aux risques. C'est aussi vérifier que les procédures et les exigences du Groupe sont bien déployées dans les filiales et succursales, ce qui signifie disposer d'une cartographie des documents.

Ces méthodes de pilotage du risque, si elles relèvent a priori du reporting interne, peuvent requérir une couche d'intelligence logicielle afin d'agréger les informations de manière pertinente et d'évaluer le risque en en renforçant l'aspect qualitatif. L'utilisation des méthodes de groupes de pairs, ou la surveillance des changements de comportement, peuvent être utilisées pour identifier les dispositifs en défaut.

> AU-DELÀ DE LA CARTOGRAPHIE DES RISQUES, IL S'AGIT POUR LES ÉTABLISSEMENTS DE METTRE EN ACCORD LES DISPOSITIFS DE SURVEILLANCE AVEC LES RISQUES.

LES BESOINS EN TERMES DE SURVEILLANCE : RENFORCER L'INTELLIGENCE LOGICIELLE

Le deuxième type de besoin relève d'une surveillance LCB/FT consolidée au niveau Groupe, sur la base du référentiel des tiers et des opérations.

Le risque serait d'envisager des solutions du type « Minority Report », ce film dans lequel un logiciel permet d'arrêter les criminels avant qu'ils n'effectuent leurs méfaits, car génératrices de « bruit » plus que de pertinence.

• LE KYC GROUPE

Une piste de réflexion couramment envisagée concerne la vision Groupe d'un tiers, prenant en compte ses différents rôles (client, tuteur, ayant-droit, dirigeant ou bénéficiaire effectif…). Si un tiers fait l'objet d'une déclaration de soupçon dans un pays, l'information doit pouvoir être mise à disposition des autres pays et des autres métiers, tout en respectant les exigences de confidentialité locales. Cette surveillance consolidée permettrait de fournir aux services de sécurité financière locaux des informations pertinentes pour évaluer le risque d'un client.

Dans un deuxième temps, la mise en place d'un KYC Groupe permettrait de répondre aux exigences du GAFI et de l'UE en matière d'identification des bénéficiaires effectifs, tout en fluidifiant les processus KYC locaux.

• LA SURVEILLANCE DES TRANSACTIONS

La surveillance de l'activité peut aussi être renforcée : détection de réseaux, consolidation des informations négatives, prise en compte des enregistrements vocaux (par exemple dans la passation des ordres de bourse), génération de signaux faibles, traitement « intelligent » des listes de pays (un pays ne pose pas le même risque selon la zone géographique où l'on se situe), mots-clés, algorithmes de rapprochement, identification des changements de comportement, constitution de groupes de pairs…

Ces méthodes peuvent renforcer aussi la lutte contre le financement du terrorisme, jugée actuellement peu efficace (cf. étude ACAMS mars 2015), par exemple dans la surveillance de « zones à risque, connaissance de l'implantation physique des agences et des distributeurs automatiques…

METTRE EN ŒUVRE CES BESOINS

Depuis la collecte des données pour le reporting consolidé jusqu'à l'analyse algorithmique ou vectorielle des données, la 1ère étape consiste à lister et hiérarchiser les besoins (priorité, complexité), sans préjuger d'une solution informatique ou d'une autre (solution jetable, datacenter ou Big data ?).

Une méthode de classification des besoins qui peut être utilisée est la suivante :

- Niveau 1 : reporting consolidé
- Niveau 2 : analyse qualitative des données
- Niveau 3 : ajout d'une couche d'intelligence sur des données normées.

Ensuite, il s'agit d'étudier la mutualisation des besoins avec d'autres problématiques de sécurité financière. Si les exigences réglementaires de la LCB/FT ne recoupent pas les problématiques internes de lutte contre la fraude, les solutions peuvent converger (utilisation des référentiels tiers et opérations), et les méthodes d'analyse être réutilisées.

Notre expérience sur les contrôles de sécurité financière a montré qu'il est toujours plus pertinent de répondre aux risques par des solutions ciblées et pragmatiques. Des projets informatiques basés sur l'intelligence logicielle sont en cours de déploiement au sein des établissements, notamment dans les domaines marketing et commercial. La déclinaison des technologies utilisées pour ces métiers permet, dans certains cas, de générer des « quick wins » sans s'engager dans des projets aléatoires et très chers.

C'est pourquoi le recours aux experts métiers, connaissant la cible et les scénarios, et aux experts en nouvelles technologies de traitement de l'information peut s'avérer pertinent afin de concevoir des solutions adaptées à des besoins à court terme tout en capitalisant sur des solutions pérennes.

Laurent RENAUDOT

COMPLIANCE AND BANKING "GENERAL DATA PROTECTION REGULATION" : LES ENJEUX DU SECRET

LUTTER CONTRE LA FRAUDE OU LA CYBERCRIMINALITÉ, EN UTILISANT DES APPROCHES BIG DATA, EST L'UNE DES NOUVELLES PERSPECTIVES DE LA CONFORMITÉ BANCAIRE intégrant les nouvelles exigences de plus en plus complexes issues de multiples régulateurs. La nécessité d'une vision Groupe, impulsée par la 4ème directive, est en marche via la rationalisation des architectures informatiques au sein de la conformité.

Le Big data, par sa capacité d'exploiter d'énormes quantités de données, permet, en temps réel, d'identifier tout comportement jugé anormal pour ainsi prévenir et limiter la fraude. Les banques sont, en effet, contraintes de recueillir des informations sur leurs clients, et de les actualiser régulièrement. La réglementation sur la lutte contre le blanchiment d'argent leur impose d'être en mesure d'apprécier si les opérations de leurs clients sont en rapport avec leur niveau de vie.

Cependant, se pose en Europe les enjeux éthiques de l'exploitation des données personnelles dans le respect de la vie privée et de la liberté des individus, à la différence des États-Unis où il n'existe pas de loi cadre protégeant les données personnelles ; le gouvernement américain préférant encourager l'autorégulation, fidèle en cela à la philosophie économique sur laquelle il s'appuie.

LE RÈGLEMENT EUROPÉEN GDPR – GLOBAL DATA PROTECTION REGULATION

Avec le Règlement Européen GDPR, promulgué en décembre 2015, et applicable dès janvier 2018, le trilogue européen (Parlement, Commission et Conseil) s'est entendu sur les nouvelles règles en matière de protection des données, qui établissent un cadre moderne et harmonisé en matière de protection des données dans toute l'UE.

Il fixe les obligations des personnes qui effectuent le traitement des données et sont responsables de ce traitement. Il définit également les méthodes visant à assurer le respect des dispositions prévues ainsi que l'étendue des sanctions imposées à ceux qui enfreignent les règles. Des amendes de 4% du chiffre d'affaires mondial, et ce jusqu'à 20 millions d'euros, une déclaration sous 72h en cas de perte ou de vol de données personnelles sont autant d'obligations du nouveau règlement de protection des données personnelles.

Parmi ces dernières obligations, un nouveau concept, qui conditionne particulièrement la collecte des données, donne obligation d'assurer la « protection des données dès la conception » qui peut être désignée par le terme « Privacy by design ». Ces obligations imposent une vigilance particulière sur le stockage de ces données et la protection des serveurs.

En définitive, puisqu'on ne peut pas aujourd'hui croiser les fichiers, déposer des traceurs à d'autres fins que commerciales, la collecte des infos de masse utilisant le Big data devient complexe.

DU CADRE RÉGLEMENTAIRE FRANÇAIS…

En France, l'approche du problème est différente. Il convient de préciser ce que dit la loi sur le sujet, quelles sont les informations utilisables, et dans quel but.

La CNIL, l'ARCEP (Autorité de régulation des communications électroniques et des postes – Autorité Administrative indépendante) nous précisent les informations clients utilisables dans le strict respect de leur vie privée (Cf. Paquet Télécom de 2009 – 2009/150/CE- et loi informatique et liberté du 6 janvier 1978).

Les données personnelles (article 6 loi informatique et liberté) et la personne identifiable (art.2) sont les deux piliers sur lesquels s'appuient les communications de la CNIL.

La CNIL précise que « les données collectées ne doivent pas être recoupées avec d'autres traitements » (fichier clients ou statistiques de fréquentation d'autres sites par exemple). « Le traceur déposé (appelé également cookie – petit fichier posé sur le disque dur de l'utilisateur) ne doit servir qu'à la production de statistiques anonymes et ne doit pas permettre le suivi de la navigation sur différents sites. Il ne doit pas être conservé au-delà de 13 mois et ne doit pas être prorogé lors de nouvelles visites ».

Nous avons tous déjà été surpris, voire agacés, de remarquer certaines bannières publicitaires apparaître sur une page web que nous consultons, nous renvoyant vers un produit que nous avions étudié sur le web, quelques heures, quelques jours auparavant.

Seules les régies publicitaires disposent de la faculté de déposer des cookies dans nos navigateurs, pour les réutiliser plus tard, traçant ainsi l'historique de nos navigations sur le web, et ce dans un délai de 13 mois maximum. Réutiliser la navigation web des utilisateurs ou des clients n'est permise que dans le cadre de « rappel de publicité » pour le moment.

Alors que faire de ces données sous l'angle de la conformité ?

...À L'UTILISATION DES DONNÉES PUBLIQUES ET DES DONNÉES PERSONNELLES

L'utilisation de données semi publiques est-elle autorisée ? On entend par semi-publiques les données dites consultables dans les services administratifs, mais dont l'accès libre ne peut être autorisé pour des raisons de sécurité publique ou de protection de liberté.

Sur les réseaux sociaux, les utilisateurs ne cessent de déposer des informations sur leur vie privée, leur géolocalisation, leur réseau professionnel ou personnel, autant d'éléments significatifs pour une analyse conformité ou fraude.

Néanmoins, ces éléments en l'état actuel du droit ne sont pas exploitables automatiquement et ne peuvent être croisés avec d'autres fichiers clients détenus par la banque.

C'est pourquoi, en 2015, la France a dû, précipitamment, modifier les lois anti-terroristes relatives à la sécurité intérieure du pays pour, entre autres, pouvoir exploiter juridiquement des données collectées sur internet, sans l'acceptation expresse du principal intéressé.

PANORAMA INTERNATIONAL ET L'OUTIL PALANTIR – « LA PIERRE DE VISION » AMÉRICAINE

Aux États-Unis, Palantir Technologie (spécialisée dans l'analyse et la science des données) a développé un outil de détection de comportements atypiques en alliant intelligence artificielle et intelligence humaine - combinaison appelée « intelligence augmentée » - dérivé de son outil de lutte antiterroriste. Financé par les services de renseignements américains à ses débuts, Palantir permet d'effectuer des recherches simultanément dans des centaines de bases de données, jusqu'alors complétement cloisonnées. Cet outil a ainsi permis de détecter des fraudes fiscales et autres cas de blanchiment.

Tous les éditeurs concernés par l'analyse des données se positionnent sur les sujets de surveillance massive, en conformité avec le droit local.

Le gouvernement français a émis un appel d'offres pour le traitement massif des données, en novembre 2015, une semaine après les attentats de Paris, et Palantir a proposé sa candidature.

Dans ce cadre règlementaire où les données personnelles ne connaissent pas la même protection, les banques américaines ont la possibilité de traiter et de recouper des informations portant sur leurs clients, sans restriction.

Se crée ainsi une distorsion entre les GAFA*, banques américaines et les banques européennes, en fonction du lieu du siège social de l'entreprise et du lieu de production des données.

Le périmètre des informations, les possibilités juridiques et les analyses prédictives seront donc différentes et circonstanciées au lieu de collecte des données.

Les données européennes seront protégées tandis que leurs homologues américaines ne connaîtront pas le même sort.

* GAFA : Google, Apple, Facebook, Amazon

Laetitia MERCIER de BEAUROUVRE
Nicolas LACHKAR

LE BIG DATA N'EST PLUS UNE PROMESSE MAIS UNE RÉALITÉ

POUR RÉPONDRE AUX BESOINS LIÉS À LA CONFORMITÉ, LE RECOURS À L'UTILISATION D'UNE PLATE-FORME BIG DATA S'AVÈRE ÊTRE AUJOURD'HUI INCONTOURNABLE.

L'APPORT DE L'ÉCOSYSTÈME BIG DATA

L'écosystème Big data se caractérise par la règle dite des 4V : variété des formats de données, vélocité des traitements réalisés, volumétrie des données traitées, valeur des résultats obtenus. Par essence, cet écosystème permet de répondre de façon intéressante à la problématique de l'AML (Anti Money Laundering).

En effet, le Big data permet de croiser de façon instantanée un très grand volume de données, quels qu'en soient les formats et ce, avec des résultats particulièrement pertinents du fait des algorithmes qui sont mis en œuvre.

Ainsi peuvent être cités les exemples suivants :

- Le processus de connaissance client lors de son entrée en relation se traduit tout d'abord par tout ce qui relève de son identification : les données mêmes de son identification, le contrôle des informations d'identification de ce client et la consignation des pièces d'identification afférentes. Dans un second temps, il convient de procéder à la qualification du risque avant, de déclarer aux autorités compétentes les éventuels soupçons. Enfin, à tout instant, il faut être en capacité de pouvoir produire les preuves des contrôles opérés en cas d'audit du régulateur.

  Tout au long de la relation commerciale entre un client et l'établissement de crédit, un suivi régulier est également nécessaire. Il se concrétise par la revue des bases clients afin d'identifier le potentiel risque lié à un client du fait de son historique et des

éventuelles nouvelles informations émanant de listes de sanction, du profilage des clients et des comptes afin de marquer les éléments pouvant porter un risque.

- Le contrôle des transactions nécessite pour sa part la capacité à traiter simultanément et le plus rapidement possible de nombreuses opérations.

LE BIG DATA PERMET DE CROISER DE FAÇON INSTANTANÉE UN TRÈS GRAND VOLUME DE DONNÉES.

PRINCIPES DE FONCTIONNEMENT

De façon un peu plus détaillée, le Big data repose sur deux principes :

- La distribution du stockage qui permet de répartir une donnée en plusieurs blocs sur un ensemble d'unités de stockage et de répliquer l'ensemble des blocs. Cette distribution rend les données hautement disponibles. En termes de scalabilité, l'ajout d'unités de stockage est possible sans limite.

- La distribution des traitements qui sont scindés en différentes tâches unitaires (map/reduce) afin de tirer parti du parallélisme des unités de stockage / calcul et d'effectuer les traitements au plus près de la donnée. Une bonne résilience est garantie : les traitements sont ainsi rejouables sur l'ensemble du cluster. L'ajout d'unités de calcul est également possible sans limite améliorant la scalabilité des traitements.

Adossées à ces évolutions en termes de distribution de stockage et de traitement, plusieurs grandes tendances sont observées :

- une Business Intelligence de plus en plus agile grâce à une évolution du marché vers des fonctions d'analyse, de visualisation de données et de self-service ; demain un utilisateur non averti pourra ainsi manipuler des traitements statistiques complexes sans même le savoir ;

- un regain d'intérêt pour l'apprentissage automatique et pour le recours au langage naturel. Avec la montée en puissance des infrastructures, les applications utilisant (souvent conjointement) les technologies de machine learning (algorithmes capables de se corriger et d'évoluer) et le traitement du langage naturel se multiplient. Le marché, restreint aujourd'hui à des solutions très spécifiques pour développeurs experts, a un avenir certain à travers des solutions packagées prêtes-à-l'emploi afin de satisfaire des besoins opérationnels d'analyse.

L'écosystème Big data est suffisamment mature et les coûts des distributions et du stockage sont suffisamment bas pour que ces technologies soient incluses dans les progiciels du marché. Il est ainsi évident que ces technologies seront demain au cœur des systèmes orientés AML.

LES LIMITES

Néanmoins ces technologies ne seront pas utilisées, a priori, au maximum de leur capacité du fait des contraintes juridiques qui pèsent sur le mode de fonctionnement des organismes bancaires.

En effet, le respect des règlementations impose un cloisonnement des données à l'opposé de la philosophie et de la capacité à corréler.

De plus, les obligations de moyens plus que de résultats, n'incitent pas les acteurs de la place à innover plus fortement.

Enfin sur les aspects sécurité, certains mécanismes restent difficiles à mettre en œuvre pour garantir un cloisonnement logique et un aspect sécurisé aux données stockées, lorsque l'on cherche à accéder à ces données depuis le datalake.

Malgré ces différentes limites, le combat est gagné d'avance. Ces technologies s'imposent d'ores et déjà !

Emmanuel ARNAUDIN

LES CHIFFRES CLÉS

10 MILLIONS €

La plus forte amende infligée et rendue public, en France à la Banque UBS pour des faits de fraude et de blanchiment - juin 2013

9,75 MILLIONS €

Infligée par le Régulateur Anglais (FCA) pour des faits de blanchiment à la SBKJ - janvier 2013

4,6 X

L'amende infligée à HSBC pour blanchiment d'argent provenant du trafic de drogue en août 2015 s'élève à 9 milliards de dollards : c'est plus de 4,6 fois l'amende infligée à Commerzbank en mars 2015 pour des faits similaires

6 MILLIARDS €

Infligée à la BNPP par le régulateur US en mai 2014 pour violation d'embargo américain

Sources : https://www.prisonlegalnews.org/news/2015/aug/31/british-banking-giant-fined-laundering-mexican-drug-money-through-us-banks/
http://nypost.com/2015/03/12/us-slaps-germanys-commerzbank-with-1-45b-money-laundering-fine/
http://uk.reuters.com/article/uk-standardbank-fine-idUKBREA0M0LF20140123
http://www.lemonde.fr/ameriques/article/2014/06/30/la-bnp-devra-regler-8-834-milliards-de-dollars-d-amende-aux-etats-unis_4448280_3222.html

AGENDA

20.05.2016

Atelier sur les Blockchains en partenariat avec Revue banque

23.06.2016

Club Banque sur les nouveaux enjeux de la conformité

L'OFFRE SOLUCOM

UNE RÉPONSE GLOBALE, DÉDIÉE À LA CONFORMITÉ ET SÉCURITÉ FINANCIÈRE.

DIAGNOSTIQUER

- Plans de remédiation
- Cartographie des risques et contrôles
- Audit / diagnostic du dispositif : organisation, procédures, risques, outils
- Examen de dossiers KYC et analyse de transactions

DÉPLOYER

- Organisation de la fonction (groupe / filiales / local et international)
- Approche par les risques
- Reportings et échanges d'informations
- Rédaction de procédures et identification des contrôles clés

OUTILLER

- Accompagnement au choix d'un outil de surveillance des transactions ou de filtrage des flux
- Déploiement de la solution
- Expertises sur les nouvelles solutions technologiques (data analysis, big data...)
- Accompagnement au changement

ACCOMPAGNER

- Actualisation annuelle des dispositifs
- Veille règlementaire et analyse d'impact des nouveaux textes
- Formalisation du reporting Banque centrale
- Accompagnement dans le cadre de missions d'inspection des autorités de supervision

FORMER

- Communication et actions de sensibilisation
- Conception et animation de formations

INNOVER

- Nouveaux business / pratiques (fintech, digital...)
- Nouvelles technologies de filtrage et profilage
- Data science (géolocalisation, profilage, réseaux..)

Venez découvrir nos expertises Banque et Finance.

@bankobs

www.solucom.fr

Responsable de la publication : Olivier Schmitt - Rédacteur en chef : Laetitia Mercier de Beaurouvre
Contributeurs : Olivier Schmitt, Laurent Renaudot, Laetitia Mercier de Beaurouvre, Nicolas Lachkar, Emmanuel Arnaudin.
Imprimeur : Jolly - l'impression créative - Mise en page : Mélinée Gérin - Conception : Les enfants gâtés
Illustrations : © Fotolia / P5 © Samuel Zeller

solucom

Tour Franklin, 100-101 Terrasse Boieldieu,
92042 Paris La Défense Cedex
Tél. : 01 49 03 20 00
www.solucom.fr

ISBN : 978-2-918872-31-3 / EAN : 9782918872313