Yvon Avenel

Journaliste
Éditeur de
SmartcardsTrends

ANTI-BLANCHIMENT

Les SI des banques sont en première ligne

Les grands éditeurs proposent désormais des solutions logicielles spécifiques à la lutte anti-blanchiment, s'intégrant au SI de la banque. La nécessité d'automatiser les opérations de détection des mouvements atypiques et la production des alertes s'est fait sentir sous la pression réglementaire, mais aussi pour des raisons de volumétrie.

1991, 2001, 2005... Le rythme de publication des directives européennes sur le blanchiment des capitaux et le financement du terrorisme s'est brutalement accéléré. À tel point que dans ses commentaires du projet de la 3e directive européenne qui lui a été soumis fin 2005, le Comité économique et social européen (CESE) s'étonnait de voir cette directive apparaître avant qu'on ait pu même établir le bilan de la précédente. Conçue pour s'aligner sur les recommandations révisées, en 2003, du GAFI (Groupe d'action financière ou FATF, *Financial Action Task Force*) [1], cette directive entend répondre à des évolutions récentes dans les méthodes et les typologies de blanchiment, très liées d'ailleurs aux contre-mesures déjà mises en place. C'est l'un des effets paradoxaux de l'inévitable course-poursuite qui est engagée. Y aurait-il urgence ? "*Oui*", répond Chantal Cutajar, enseignante à l'université de Strasbourg, à l'origine d'un diplôme universitaire de prévention de la fraude et du blanchiment (*encadré 1*), récemment invitée d'une conférence sur le sujet à l'Atelier BNP Paribas. Et de pointer l'ampleur des dangers et menaces que représente la constitution d'une économie souterraine, nourrie par le crime organisé qui pèserait déjà 15 % du commerce mondial (quelque 800 milliards de dollars) [1]. Le préambule de la 3e directive européenne confirme le diagnostic : il évoque de la même façon les menaces que constituent les opérations de blanchiment qui remettent "*en cause des fondements même de notre société*" et précise qu'il y va également de la stabilité et de la réputation du secteur financier. Les banques sont évidemment en première ligne... mais aussi en première ligne de défense. "*Les banques sont et resteront les plus exposées, mais aussi les mieux protégées*", confirme Alain Damais, le secrétaire exécutif du GAFI qui constate "*l'impressionnant travail déjà réalisé et l'expertise développée par le secteur bancaire, dans la plupart des pays membres du GAFI, pour lutter avec des résultats déjà tangibles contre les opérations de blanchiment.*" Certains de ces résultats peuvent d'ailleurs se voir dans la part croissante prise par les opérations de blanchiment à partir de transferts physiques d'argent liquide (*cash courriers*) et le recours à des officines plus ou moins occultes pour ces transferts hors des circuits bancaires. Quoi qu'il en soit, cette accélération des initiatives réglementaires et ce branle-bas de combat ne sont pas propres à l'Europe dont la 3e directive doit être normalement transposée dans tous les pays d'Europe le 15 décembre 2007. La publication dans la période de l'après 11 septembre 2001 des 8 recommandations spéciales du GAFI sur le financement du terrorisme (en octobre 2001), du *USA Patriot Act* aux États-Unis (2003), puis la révision, en 2003 également, des 40 recommandations du GAFI, suivie par celle de ses 9

> *« Les efforts de régulation internationaux ont favorisé l'éclosion d'une industrie de la conformité et de solutions logicielles spécifiques à la lutte anti-blanchiment. »*

FORMATION

Un diplôme universitaire dédié à la prévention des fraudes et du blanchiment

Issu d'une initiative conjointe de l'université de Strasbourg et du service central de la prévention de la corruption, le diplôme universitaire "Prévention des fraudes et du blanchiment" a pour objectif de former des experts maîtrisant le cadre juridique, technique, économique et comptable des montages dans lesquels s'inscrivent la fraude, la corruption, le financement du terrorisme, le blanchiment et permettant, en outre, le développement du crime organisé.
Douze modules sont prévus, dont trois en présentiel. Le plus important, "Analyses et montages", représente 120 heures de cours.
Admission : master 1 et maîtrise.
Le démarrage de la formation est prévu en février 2007.

2. RECOMMANDATIONS

Devoir de vigilance à l'égard du client et connaissance du client

■ Le devoir de vigilance – renforcée ou simplifiée – à l'égard de la clientèle, figure en bonne place dans les 40 recommandations du GAFI (R5 à R12), et trouve également une place de choix dans la directive européenne (section 2 et section 3). C'est également l'un des leitmotivs de la section 326 de l'*USA Patriot Act* (*due diligence*), et des directives mondiales du groupe Wolfsberg. Cette convergence de vue établit le fameux impératif KYC (*Know Your Customer*) comme l'une des clés de la lutte contre le blanchiment. Mais certains remarquent que la notion de client n'est pas aussi aisée à cerner qu'il n'y paraît, si tant est que sa vision, pour les banques, reste souvent comptable (son profilage est établi au travers de son comportement financier), que son unicité (la vue unique idéale du CRM) n'est pas toujours bien assurée au travers des différents systèmes de gestion du même établissement, et que son identité n'est pas toujours formellement prouvée. Elle l'est d'ailleurs d'autant moins que le nombre de cas où le client n'est plus présent est en forte croissance, et que le vol d'identité reste l'un des crimes dont l'évolution est la plus préoccupante [1].

La vigilance à l'égard de la clientèle peut supposer en outre des investigations dans l'identification des personnes physiques ou morales que la troisième directive qualifie de "plus rigoureuses" que les autres, ou le recours à des listes (PPE, personnes politiquement exposées) pour évaluer les risques, qui pourraient, dans certains cas, entrer en conflit avec des législations sur la protection de la vie privée. Une délibération de la CNIL, publiée en mars 2006, précise ainsi le cadre de la loi sur le sujet. Elle porte sur "*l'autorisation unique de certains traitements de données à caractère personnel mis en œuvre par des organismes financiers au titre de la lutte contre le blanchiment des capitaux et le financement du terrorisme*." Certains de ces traitements, dont l'autorisation est strictement associée à des établissements du secteur bancaire, sont néanmoins soumis à des autorisations au cas par cas. Pour répondre à ces différentes questions, on peut noter qu'il existe aujourd'hui des solutions logicielles, mais aussi – on commence à le voir en Belgique qui est le premier pays européen à s'être doté d'une carte d'identité électronique –, des solutions plus institutionnelles qui créent un nouvel environnement de confiance, en particulier pour l'identification des personnes.

La suite logicielle EAS (*Entity Analytic Solution*) d'IBM, qui tourne avec une base de données DB2, divisée en trois modules [2], est ainsi une solution KYC très orientée sur les données "extra-comptables" (qui connaît qui ? qui est qui ? à partir des données associées au compte), qui s'attache à résoudre des problèmes d'identité multiples, mais également à préserver l'anonymat des informations utilisées. Le logiciel peut traiter jusqu'à 2000 identités à la seconde et reconnaître une personne physique ou morale parmi plusieurs identités, par association transitive d'attributs : tel numéro de téléphone permet de confondre deux personnes A et B, puis B et C, par une adresse postale, puis encore C et D, par un visage, etc. Le système peut ainsi travailler sur une quinzaine d'entités séparées par des attributs différents, mais en partie communs. Le système dispose de capacités d'autocorrection qui sont liées à sa taille et au nombre de ses enregistrements (ils sont tous conservés dans la base de travail) : plus il y a d'identités analysées, plus le système devient précis (le nombre de faux positifs décroît).

La collecte de l'information sur la clientèle et l'identification des clients au sens où l'entend la 3e directive européenne posent d'autres problèmes et suggèrent que les solutions sont avant tout liées à des pratiques nouvelles et à des sensibilités culturelles. L'exemple donné par le Crédit Agricole (Landbouwkrediet) en Belgique, qui vient de s'équiper d'un système anti-blanchiment très intégré, est en cela assez édifiant. Pour Koen de Vits, Resources, Organisation & Operations, Landbouwkrediet, (*voir l'interview*), la difficulté à collecter des informations sur la clientèle, est aujourd'hui beaucoup plus ressentie par les commerciaux de la banque "*qui craignent de gêner leurs clients en les sollicitant avec des questions qui pourraient être considérées comme indiscrètes*" que par les clients eux-mêmes qui ont admis la nécessité de cette démarche. Une attitude que l'on peut sans doute rapprocher de celle qui a accompagné la mise en place en Belgique de la première carte d'identité électronique, maintenant totalement acceptée et utilisée au moment de l'ouverture d'un compte, ou d'une demande de crédits, avec un confort et une confiance bien plus grande – sur Internet notamment – qu'auparavant lorsqu'il fallait produire des photocopies des cartes d'identité. "*C'est plus sûr, et ça va beaucoup plus vite*", souligne Koen de Vits.

(1) Selon une étude Datamonitor conduite en janvier 2006 à partir d'interviews auprès de responsables de grandes banques et services financiers internationaux, le vol d'identité (87 %) et le blanchiment (86 %) sont les deux crimes financiers les plus préoccupants.
(2) Le premier module est une suite dédiée à la résolution d'identité, à travers des silos de données, selon tous les critères possibles. La seconde est une suite qui reconnaît les relations évidentes ou non entre des personnes et des groupes, avec des alertes instantanées au moment de l'enregistrement d'un nouveau nom, et enfin la troisième est un module, qui permet de partager des données personnelles de façon anonyme.

recommandations spéciales visant le financement du terrorisme – maintenant acceptées et mises en œuvre par 172 pays – ont créé ces dernières années une pression réglementaire croissante, renforcée par celle des autorités de tutelle dans chaque pays (en France : AMF, Commission bancaire, etc.). Il faudrait ajouter à cela le rôle joué par les travaux réguliers que le GAFI a engagé, par ailleurs, sur l'analyse des typologies et des méthodes utilisées par les blanchisseurs dans le domaine des transactions commerciales, des nouveaux moyens de paiement, ou dans la constitution de trusts ou d'entités juridiques, mais aussi les travaux qui permettent des évaluations mutuelles par pays des mesures prises contre le blanchiment et le financement du terrorisme.

Globalement, l'ensemble de ces mesures et de ces travaux soulignent pour les secteurs d'activité concernés, la nécessité de développer en interne des politiques, des procédures de contrôle et des moyens de gestion des risques, de façon à prévenir ou détecter des opérations de blanchiment, de désigner une personne responsable (*compliance and risk officer*) de ce programme et de son fonctionnement, d'apporter la formation idoine pour les équipes en charge de ce programme, et enfin d'assurer l'audit et la validation de ce dernier par un organisme extérieur indépendant.

LA NAISSANCE D'UNE INDUSTRIE DE LA CONFORMITÉ

Dans le détail, les orientations récentes (notamment celles de la 3e directive européenne, mais aussi la section 326 du USA

Patriot Act) pointent l'importance des procédures et des moyens mis en place pour améliorer la connaissance du client et l'identification de son activité (*encadré 3*), mais aussi les ressources affectées à la conservation des historiques des opérations et des documents d'identification fournis. De surcroît, elles mettent toutes en évidence la globalité des problèmes posés par le blanchiment et les liens qui existent naturellement entre tous les types de fraudes (le financement du terrorisme, notamment) et les opérations de blanchiment. Un constat qui se traduit dans les textes les plus récents par une extension des domaines d'applications de la loi, et une extension des déclarations de soupçon à des infractions sous-jacentes comme la fraude fiscale ou à des infractions graves (peine punissable d'un an d'emprisonnement dans la 3e directive) dont les implications en termes de volumétrie, de formation (juridique) des personnes ou de traitement, mais aussi de responsabilité et d'évaluation du risque sont loin d'être triviales. Autant dire que les termes du problème posé par la lutte contre le blanchiment ont fondamentalement changé en quelques années. Les impacts sur les organisations, sur la fonction "conformité", et sur les systèmes d'informations (SI) des entreprises concernées sont devenus structurants. "*Indéniablement, les efforts de régulation internationaux ont favorisé l'éclosion d'une industrie de la conformité et de solutions logicielles spécifiques à la lutte anti-blanchiment*", indique Alain Damais. Aujourd'hui, une solution anti-blanchiment se compose assez classiquement d'un ensemble d'outils logiciels modulaires : des outils de contrôle au moment de l'ouverture d'un compte (SIDE, Factiva Fircosoft proposent ainsi des outils de filtrage et de gestion de risque associée aux listes PPE ou aux listes OFAC), des outils de profilage des comptes et des clients (SAS AML, Searchspace, Neteconomy, ACI, Mantas), des outils de détection des transactions atypiques (ACI, Searchspace, Mantas, Neteconomy, SAS), et enfin des outils de *workflow*, et de suivi des alertes qui peuvent intégrer des outils de *reporting* et des moyens de transmissions automatiques et sécurisés vers les autorités compétentes dans chacun des pays pour traiter les déclarations de soupçon (en France : TracFin, etc.). Mais, dans bien des cas, les grands éditeurs du domaine, soit seuls, soit avec des partenaires, proposent des solutions complètes, portables sur des serveurs spécialisés Windows ou Unix et dotés d'outils ETL pour s'intégrer au SI de la banque, et communiquer avec d'autres applications.

PUISSANCE DE CALCUL, FINESSE DE L'ANALYSE

La nécessité d'automatiser les opérations de détection des mouvements atypiques et la production des alertes s'est fait sentir sous cette pression réglementaire, mais aussi pour de simples raisons de volumétrie. La Barclays Bank UK, par exemple, qui s'est équipée en 2001 d'un centre anti-blanchiment (AML Center) de 30 analystes et d'un logiciel de filtrage, d'analyse et de détection (Searchspace), traite 16 millions de transactions par jour. Chaque analyste gère en moyenne 700 000 comptes. Même s'il subsiste des traitements purement "manuels" issus des agences, la banque ne pouvait faire face à une telle volumétrie sans l'aide outils et de solutions intégrées à son système d'information. Cette évolution vaut pour des organisations de taille plus modeste.

"*Le temps réel, 24 h/24, est devenu un passage obligé de façon à analyser au fil de l'eau et à réagir le cas échéant très vite, bloquer la transaction ou lancer une enquête. Cela impose évidemment des moyens de calcul adaptés à la volumétrie à traiter, mais aussi à ses caractéristiques. Celles-ci réclament une finesse dans l'analyse et le recours à des règles expertes. L'automatisation s'impose maintenant partout*", souligne David Destemberg, responsable des solutions Banque, Finance et Assurance chez SAS France, qui note, par ailleurs, "*à quel point la donne a pu changer au cours des cinq dernières années à cause de la mondialisation, de la part croissante prise par Internet et la montée en puissance de la banque en ligne*". Le facteur "temps" est devenu essentiel : des transactions portant sur de gros montants, devenues trop "visibles", sont désormais souvent éclatées en petites transactions effectuées dans un temps record. "*L'analyse des transactions repose sur des règles expertes qui prennent en compte la vélocité et l'origine des mouvements, mais font aussi appel à des technologies comme les réseaux neuronaux ou la logique floue qui permettent de faire de l'analyse comportementale capable de déceler des attitudes atypiques, en se référant à des historiques et à des modèles d'appartenance à tel ou tel type de groupe (Peer Groups)*", indique Jean-Michel Schneider, représentant pour la France d'ACI Worldwide.

> *« La Barclays Bank UK, par exemple, qui s'est équipée en 2001 d'un centre anti-blanchiment de 30 analystes et d'un logiciel de filtrage, d'analyse et de détection, traite 16 millions de transactions par jour. »*

PARVENIR AU MEILLEUR RATIO TRANSACTIONS/ALERTES

"*Les meilleures solutions d'automatisation sont celles qui sont basées sur des systèmes itératifs d'auto-apprentissage, capables de corriger finement avec le temps et l'expérience, les scénarios sous-jacents qui servent à déclencher les alertes*", souligne Rosemary Turley, directrice du marketing de Norkom Technologies. L'enjeu est bien sûr d'éviter l'asphyxie sous une avalanche d'alertes. "*Il n'y a pas de ratio type idéal*", indique la directrice de Norkom, mais on sait réduire le nombre des "fausses positives", avec le temps, en excluant les personnes ou les comptes qui ont déjà été l'objet d'enquêtes approfondies, par exemple, ou en excluant les transactions

3. TRANSPOSITION

Encore un an pour transposer la 3e directive européenne

■ Un peu plus d'un an encore pour anticiper la loi de transposition de la troisième directive européenne. Certains pays européens, comme le Grande-Bretagne ou la Belgique, n'ont pas attendu les mesures d'exécutions qui devaient être prises au niveau européen en juin dernier, pour transposer la loi ou en tout cas, avancer la date de sa transposition fixée au plus tard au 15 décembre 2007. En France, ces mesures d'exécution étaient attendues en juillet afin d'engager le processus de concertation interministériel puis interprofessionnel, avant d'aller plus avant dans la préparation de la loi de transposition.

Les outils et suites logiciels dédiés à la lutte anti-blanchiment

Nom	Fonction	Fournisseur	Remarques
SafeWatch	Filtrage, gestion de listes noires et de risque associé	SIDE	
OPAC-Agent	Filtrage, gestion de listes noires et de risque associé	FircoSoft	
PEP Risk Score	Filtrage, gestion de listes noires et de risque associé	Factiva	
Searchspace Intelligent Enterprise Framework	Suite complète du filtrage au *workflow*	Searchspace	Architecture J2EEE, intégrant une base de données DB2. Les modules applicatifs (anti-blanchiment, fraude à la carte bancaire, ATM, conformité, etc.) baptisés Sentinel peuvent être ajoutés à la demande
SAS AML	Suite complète du filtrage au *workflow*	SAS	Architecture modulaire. Cinq modules indépendants
ERASE AML Solution	Suite complète du filtrage au *workflow*	Neteconomy	
Norkom Platform	Suite complète du filtrage au *workflow*	Norkom	Cette plate-forme a vocation à traiter tous les types de fraudes
ACI Proactive Risk Manager for AML	Suite complète du filtrage (partenaire) au *workflow*	ACI Worldwide	Architecture modulaire
Actimize Anti-Money Laundering Solution	Détection des comportements à risque (comptes, transactions et clients)	Actimize	D'autres fonctions (*workflow*, profilage, *reportings*, etc.) sont fournies par ailleurs
Mantas Behaviour Detection Platform	Détection des comportements à risque (comptes, transactions et clients)	Mantas	
EAS (*Entity Analytic Solutions*)	KYC, résolution d'identité	IBM	Architecture modulaire avec DB2. Quatre modules

en dessous d'un certain seuil [3]. La banque KBC est parvenue ainsi à réduire de 2 000 à 600 le nombre de ses alertes par jour, par un fin réglage des paramètres des scénarios de son système de détection. La banque gère aujourd'hui ce niveau d'alerte avec 4 personnes, pour 400 000 transactions par jour. "*Il en aurait fallu 20 pour répondre en « manuel » à cet afflux d'alertes*", souligne Bruno Van den Meerschaut, responsable chez KBC de la lutte anti-blanchiment.

GLOSSAIRE

PPE : personnes politiquement exposées (ou PEP *politically exposed person*). Ces personnes doivent faire l'objet d'une vigilance renforcée. Des outils existent qui gèrent des listes et calculent le risque associé.
OFAC : *US Office of Foreign Assets Control*. Organisme américain qui établit des listes de pays, de sociétés ou de personnes réputés à risque en matière de blanchiment et dont les transactions doivent être bloquées.
***Peer group* :** groupe de clients classés à partir d'attributs communs comme le lieu de résidence, les revenus, des éléments de style de vie, et qui servent à établir des profils types, lesquels vont permettre ensuite, par comparaison, d'identifier des comportements atypiques.
Profilage : méthode qui permet de tracer des modèles de comportement financiers d'un client à partir de l'historique des mouvements de son compte, et qui permettra de reconnaître des anomalies, le cas échéant.

Mais l'enjeu est tout aussi bien d'éviter les "fausses négatives" et de s'assurer que toutes les alertes ont bien été traitées, et qu'elles sont bien conservées pour servir de base à des analyses ultérieures. La solution Searchspace, mise en œuvre par la Barclays qui permet de traiter jusqu'à 20 millions (en pics) de transactions sur 24 heures, est ainsi – comme la plupart des suites proposées sur le marché – inséparable d'un *workflow* qui permet de gérer le volume d'alertes (environ 500 par jour), de les tracer individuellement. Ce *workflow* est également relié à un système d'archivage. Ce dernier stocke ainsi toutes les alertes identifiées depuis 12 ans.

Les outils et les suites anti-blanchiment gagnent à être le plus intégrés possible au système d'information de la banque. Rosemary Turley (Norkom Technologies) note qu'il y a désormais un grand bénéfice à penser la lutte contre la fraude de façon globale, et défend du coup, son concept de plateforme technique. "*On ne peut pas séparer les attaques physiques contre les banques, de la fraude à la carte bancaire ou aux ATM, du blanchiment.*" Les logiciels utilisent d'ailleurs les mêmes données, les mêmes *workflows*, des systèmes de gestion des risques, de *scoring*, de profilage similaires. Jean-Michel Schneider (ACI) souligne que d'un simple point de vue ergonomique, cette intégration est nécessaire : "*Quand il s'agit de lancer une enquête pour répondre à une alerte, et savoir rapidement la conduite à tenir, il est important d'avoir toutes les données utiles sous la main.*" En Belgique, le groupe Crédit Agricole a su marier sa solution anti-blanchiment et son CRM, sans qu'il y ait pourtant confusion des genres. "*Parce que les cycles d'analyse et de profilage dans la base CRM sont plus rapides que ceux de la base AML, nous ne pouvons utiliser qu'une partie de la base AML pour le CRM, mais pas l'inverse*", remarque Koen de Vits. ■

NOTES

[1] Il s'agit d'une évaluation difficile à recouper. Selon le GAFi, il n'est pas possible de donner aujourd'hui de chiffres fiables sur le volume et les montants des opérations de blanchiment. Les chiffres qui circulent partout – entre 2 et 5 %, soit entre 750 et 1 750 milliards de dollars – du PIB mondial, sont issus de travaux faits par un économiste du FMI en 1995, et qui sont révisés mécaniquement d'année en année en fonction de l'évolution du PIB. Une étude datant de 4 ans fait état d'un taux de croissance de 2,7 % par an des montants "blanchis" (A Brave New World for Financial Institutions - Celent Report 2002).
[2] L'organisme international de normalisation dans le secteur de la lutte contre le blanchiment de capitaux et le financement du terrorisme.
[3] La troisième directive a fixé ce seuil à 15 000 euros. Il est de 10 000 dollars pour l'USA Patriot Act.